KASPERSKY LAB

Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition

ADMINISTRATOR-HANDBUCH

KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS
ENTERPRISE EDITION

Administratorhandbuch

http://www.kaspersky.com/de

Version: Juli 2008

Inhalt

KAPITEL 1. VORWORT

Dieses Handbuch beschreibt den Umgang mit dem Programm **Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition** (im Weiteren als "Anti-Virus" bezeichnet).

Abschnitt 1.1 auf S. 13 enthält allgemeine Informationen über Anti-Virus sowie eine Beschreibung seiner Funktionen und der erkennbaren Bedrohungen.

In Teil 1 des Handbuchs, *Konfiguration und Verwaltung über die MMC-Konsole* steht, wie Anti-Virus über die Konsole, die auf einem geschützten Server oder einer Remote-Workstation installiert ist, verwaltet wird.

Wie Anti-Virus aus der Befehlszeile eines geschützten Servers verwaltet wird, erfahren Sie in Teil 2, *Verwaltung von Anti-Virus aus der Befehlszeile*.

Teil 3, *Konfiguration und Verwaltung über Kaspersky Administration Kit*, beschreibt, wie der Schutz von Servern, auf denen Anti-Virus installiert ist, mit Hilfe von Kaspersky Administration Kit zentral verwaltet wird.

In Teil 4, *Anti-Virus-Counter* werden die Counter von Anti-Virus für die Anwendung **Systemmonitor** sowie SNMP-Counter und -Schwachstellen beschrieben.

Sollten Sie in diesem Dokument keine Antwort auf Ihre Frage über Anti-Virus gefunden haben, dann können Sie weitere Informationsquellen verwenden (s. Pkt. 1.2 auf S. 20).

1.1. Allgemeine Informationen zu Anti-Virus

Anti-Virus schützt Server auf der Plattform Microsoft Windows vor Bedrohungen, die bei der Übertragung von Dateien eindringen können. Er dient dem Einsatz in lokalen Netzwerken mittlerer und großer Unternehmen. Die Benutzer von Anti-Virus sind Netzwerkadministratoren und Mitarbeiter, die für die Antiviren-Sicherheit zuständig sind.

Sie können Anti-Virus auf Servern installieren, die unterschiedliche Funktionen erfüllen: Terminalserver und Printserver, Anwendungsserver und Domänen-Controller, sowie Dateiserver, die dem höchsten Infektionsrisiko unterliegen, weil Dateien mit Benutzer-Workstations ausgetauscht werden.

Es bestehen mehrere Möglichkeiten, um den Schutz des Servers, auf dem Anti-Virus installiert ist, zu verwalten: über die Anti-Virus-Konsole in der MMC, über die Befehlszeile sowie unter Verwendung der Anwendung Kaspersky Administra-

tion Kit, die der zentralisierten Verwaltung des Schutzes mehrerer Server dient, auf denen Anti-Virus installiert ist. Sie können die Produktivitäts-Counter von Anti-Virus für die Anwendung **Systemmonitor** sowie SNMP-Counter und -Schwachstellen anzeigen.

Dieser Abschnitt enthält Informationen:

- über die Anti-Virus-Funktionen *Echtzeitschutz* und *Virensuche* (s. Pkt. 1.1.1 auf S. 14)
- über die Bedrohungen, die von Anti-Virus erkannt und neutralisiert werden (s. Pkt. 1.1.2 auf S. 15).
- darüber, wie Anti-Virus infizierte, verdächtige und potentiell gefährliche Objekte aufspürt (s. Pkt. 1.1.3 auf S. 19).

1.1.1. Echtzeitschutz und Virensuche

Zum Schutz von Servern können Sie zwei Funktionen des Anti-Virus verwenden: *Echtzeitschutz* und *Virensuche*. Sie können diese Funktionen manuell und nach Zeitplan aktivieren und deaktivieren.

Der **Echtzeitschutz** wird automatisch beim Start von Anti-Virus gestartet und arbeitet ununterbrochen.

Anti-Virus untersucht die folgenden Objekte des geschützten Servers, wenn darauf zugegriffen wird:

- Dateien
- alternative Datenströme der Dateisysteme (NTFS-Streams)
- Hauptbooteintrag und Bootsektoren der lokalen Festplatten und Wechseldatenträger

Wenn ein Programm eine Datei auf den Server schreibt oder sie ausliest, fängt Anti-Virus diese Datei ab, untersucht sie auf Bedrohungen und wenn er eine Bedrohung erkennt, führt er die von Ihnen vorgegebenen Aktionen aus: Er versucht, die Datei zu desinfizieren, oder löscht sie. Anti-Virus gibt die Datei nur an das Programm zurück, wenn sie virenfrei ist oder erfolgreich desinfiziert wurde.

Anti-Virus untersucht Objekte nicht nur auf Viren, sondern auch auf andere Bedrohungstypen wie beispielsweise trojanische Programme, Adware und Spyware. Details zu den Bedrohungen, die Anti-Virus aufspürt und unschädlich macht, finden Sie in Pkt. 1.1.2 auf S. 15.

Außerdem überwacht Anti-Virus auf einem geschützen Server ständig alle Versuche zum Ausführen von Skripts der Typen VBScript und JScript, die mit Microsoft Windows Script Technologies (oder Active Scripting) erstellt wurden. Er un-

tersucht den Programmcode der Skripts und verbietet automatisch die Ausführung gefährlicher Skripts.

Der Echtzeitschutz des Servers vor Viren soll bei minimaler Verzögerung des Dateiaustauschs für maximale Sicherheit des Servers sorgen.

Die **Virensuche** ist eine einmalige vollständige oder benutzerdefinierte Untersuchung von Serverobjekten auf Bedrohungen.

Anti-Virus untersucht Dateien, den Arbeitsspeicher des Servers sowie Autostart-Objekte, die sich nur schwer wiederherstellen lassen, wenn sie beschädigt wurden.

In der Grundeinstellung führt Anti-Virus die Aufgabe zur vollständigen Untersuchung des Computers einmal pro Woche aus. Es wird empfohlen, die Virensuche manuell zu starten, wenn der Echtzeitschutz für Dateien deaktiviert wurde.

1.1.2. Bedrohungen, die Anti-Virus erkennt

Anti-Virus kann in Objekten des Dateisystems hunderttausende verschiedener Schadprogramme erkennen. Einige schädliche Programme stellen eine große Gefahr für den Benutzer dar, andere sind nur unter bestimmten Bedingungen riskant. Wenn Anti-Virus einen Schädling findet, wird dieser entsprechend seiner Gefahrenstufe (hoch, mittel und niedrig) einer bestimmten Kategorie zugeordnet.

Anti-Virus unterscheidet folgende Kategorien von Schadprogrammen:

- Viren und Würmer (Virware)
- trojanische Programme (Trojware)
- sonstige Schadprogramme (Malware)
- Programme mit pornografischem Inhalt (Pornware)
- Werbeprogramme (Adware)
- potentiell gefährliche Programme (Riskware)

Hinweis

Die Gefahrenstufe der Bedrohungen in gefundenen verdächtigen Objekten wird im Knoten **Quarantäne** (Kapitel 11 auf S. 170) genannt; die Gefahrenstufe von Bedrohungen in infizierten Objekten im Knoten **Backup** (Kapitel 12 auf S. 189).

Eine kurze Beschreibung der Bedrohungen folgt unten. Ausführliche Informationen zu schädlichen Programmen und eine Malware-Klassifikation finden Sie in der Viren-Enzyklopädie von Kaspersky Lab (http://www.viruslist.com/de/viruses/encyclopedia).

Viren und Würmer (Virware)

Gefahrenstufe: hoch

Diese Klasse umfasst klassische Viren und Netzwerkwürmer.

Ein **klassischer Virus** (Klasse Virus) infiziert Daten oder Dateien anderer Programme. Er fügt ihnen seinen Code hinzu, um beim Öffnen die Kontrolle zu übernehmen. Ist ein klassischer Virus in ein System eingedrungen, dann wird er durch ein bestimmtes Ereignis aktiviert und führt seine schädlichen Aktionen aus.

Klassische Viren werden nach ihrem Milieu und der Infektionsmethode unterschieden.

Unter *Milieu* versteht man Bereiche eines Computers, Betriebssysteme oder Programme, in die sich der Virencode eindringen kann. Nach dem Milieu werden Dateiviren, Bootviren, Makroviren und Skriptviren unterschieden.

Unter *Infektionsmethode* versteht man verschiedene Methoden des Eindringens von Virencode in infizierbare Objekte. Im Hinblick auf die Infektionsmethoden existiert eine Vielzahl unterschiedlicher Virentypen. *Überschreibende* Viren (Overwriting) schreiben ihren Code an die Stelle des Codes der infizierten Datei und zerstören ihren Inhalt. Die infizierte Datei verliert ihre Funktionsfähigkeit und kann nicht repariert werden. *Parasitäre* Viren (Parasitic) verändern den Code von Dateien, wobei die Datei voll oder teilweise funktionsfähig bleibt. *Companion-Viren* (Companion) ändern Dateien nicht, sondern legen Zwillingsdateien an. Beim Start der infizierten Datei übernimmt der Zwilling, also der Virus die Kontrolle. Weitere Virentypen sind *Linkviren* (Link), *Viren, die Objektmodule* (OBJ), *Compiler-Bibliotheken* (LIB) *oder den Quelltext von Programmen infizieren*, u.a.

Der Code von **Netzwerkwürmern** (Klasse Würmer) wird wie der Code klassischer Viren nach dem Eindringen in einen Computer aktiviert und führt schädliche Aktionen aus. Ihre Bezeichnung geht darauf zurück, dass sie wie Würmer von Computer zu Computer "kriechen" können und ihre Kopien über verschiedene Datenkanäle verbreiten.

Das grundlegende Merkmal, nach dem Netzwerkwürmer voneinander unterschieden werden ist die Art der Weiterverbreitung. Sie werden unterteilt in *Mailwürmer*, die Internet-Messenger verwenden, *IRC-Würmer*, *Würmer in Dateitausch-Netzwerken* sowie *sonstige Netzwerkwürmer*. Zu letzteren zählen Würmer, die ihre Kopien in Netzwerkressourcen verbreiten, über Schwachstellen von Betriebssystemen und Programmen in einen Rechner eindringen, in öffentliche Netzwerkressourcen einbrechen und als Parasiten anderer Bedrohungen auftreten.

Netzwerkwürmer verfügen häufig über eine sehr hohe Ausbreitungsgeschwindigkeit.

Netzwerkwürmer schädigen nicht nur den infizierten Computer, sie diskreditieren auch dessen Besitzer, verursachen durch zusätzlichen Netzwerkverkehr finanziellen Schaden und belasten Internet-Kanäle.

Trojanische Programme (Trojware)

Gefahrenstufe: hoch

Trojanische Programme (Klassen Trojan, Backdoor, Rootkit u.a.) lösen auf Computern Aktionen aus, die vom Benutzer nicht sanktioniert wurden. Sie stehlen Kennwörter, greifen auf Internet-Ressourcen zu, laden und installieren andere Programme, usw.

Im Gegensatz zu klassischen Viren verbreiten sich trojanische Programme nicht selbständig, um in Dateien einzudringen und diese zu infizieren. Sie werden auf Befehl ihres "Besitzers" übertragen. Dabei kann der von einem Trojaner verursachte Schaden den eines traditionellen Virenangriffs erheblich übersteigen.

Als gefährlichste trojanische Programme gelten *ferngesteuerte Trojaner* (Backdoor). Wenn solche Programme gestartet werden, installieren sie sich im System, ohne dass der Benutzer es bemerkt, und übernehmen die heimliche Kontrolle: Sie zerstören Daten auf den Laufwerken, bringen das System zum Absturz und übertragen Informationen an ihren Urheber.

Eine besondere Rolle unter den trojanischen Programmen spielen Rootkits. Wie andere Trojaner dringen Sie unbemerkt in ein System ein. Sie führen keine schädlichen Aktionen aus, tarnen aber andere Malware und deren Aktivität, damit sich diese möglichst lang im infizierten System verbergen können. Rootkits können Dateien, Prozesse im Arbeitsspeicher des infizierten Computers oder Registrierungsschlüssel, die Schadprogramme starten, maskieren. Außerdem können Rootkits den Zugriff eines Angreifers auf das System verheimlichen.

Sonstige schädliche Programme (Malware)

Gefahrenstufe: mittel

Die sonstigen Schadprogramme stellen keine Bedrohung für den Computer dar, auf dem sie ausgeführt werden. Sie können jedoch zur Organisation von Hackerangriffen auf Remote-Server, zum Einbruch in andere Computer sowie zum Erzeugen anderer Viren oder Trojaner benutzt werden.

Es existiert eine Vielzahl von sonstigen schädlichen Programmen. *Netzwerkangriffe* (Klasse DoS (Denial of Service)) senden eine große Anzahl von Anfragen an Remote-Server, um auf diesen Fehlfunktionen hervorzurufen. *Böse Scherze* (Typen BadJoke, Hoax) sollen den Benutzer durch virenähnliche Meldungen erschrecken, die angeben, das eine in Wirklichkeit virenfreie Datei infiziert ist oder dass die Festplatte formatiert wird, obwohl dies nicht der Fall ist. *Chiffreure* (Klassen FileCryptor, PolyCryptor) verschlüsseln andere Schadprogramme, um sie vor Antiviren-Programmen zu verstecken. *Konstrukteure* (Klasse Constructor) erlauben es, Quelltext von Viren, Objektmodule oder infizierte Dateien zu gene-

rieren. *Spam-Werkzeuge* (Klasse SpamTool) sammeln auf einem infizierten Computer E-Mail-Adressen oder missbrauchen ihn als "Spam-Maschine".

Programme mit pornografischem Inhalt (Pornware)

Gefahrenstufe: mittel

Programme mit pornografischem Inhalt zählen zur Klasse der bedingt gefährlichen Programme (not-a-virus). Sie verfügen über Funktionen, die dem Benutzer nur unter bestimmten Bedingungen Schaden zufügen können.

Pornware-Programme zeigen Benutzern Informationen mit pornografischem Inhalt. Abhängig vom Verhalten der Programme werden drei Typen unterschieden: *Einwahlprogramme* (Porn-Dialer), *Programme zum Download von Dateien aus dem Internet* (Porn-Downloader) und *Werkzeuge* (Porn-Tools). Porn-Dialer stellen über das Modem Verbindungen mit kostenpflichtigen pornografischen Internet-Ressourcen her. Porn-Downloader laden pornografische Materialien aus dem Internet auf den Computer herunter. Zu den Porn-Tools zählen Programme, die der Suche und Anzeige von pornografischen Materialien dienen (beispielsweise spezielle Symbolleisten für Browser und spezielle Video-Player).

Werbeprogramme (Adware)

Gefahrenstufe: mittel

Adware gilt als bedingt gefährlich (Klasse not-a-virus). Solche Programme werden ohne Wissen des Benutzers in andere Software integriert und haben die Präsentation von Werbung auf der Programmoberfläche zum Ziel. Oft blendet Adware nicht nur Werbung ein, sondern sammelt auch persönliche Benutzerdaten und leitet sie an den Urheber weiter, verändert Browser-Einstellungen (Start- und Suchseiten, Sicherheitsstufe usw.) und erzeugt für den Benutzer unkontrollierbaren Datenverkehr. Durch die Aktionen von Adware kann die Sicherheitsrichtlinie verletzt werden und es können direkte finanzielle Verluste entstehen.

Potentiell gefährliche Programme (Riskware)

Gefahrenstufe: niedrig

Potentiell gefährliche Programme zählen zur Klasse der bedingt gefährlichen Programme (not-a-virus). Solche Programme können legal verkauft werden und dienen beispielsweise als gebräuchliche Werkzeuge für Systemadministratoren.

Als potentiell gefährlich gelten z.B. bestimmte Programme wie RemoteAdmin, die der Fernverwaltung dienen. Der Benutzer installiert und startet diese Programme selbst auf seinem Computer. Das unterscheidet sie von ferngesteuerten Backdoor-Trojanern, die sich selbst im System installieren und agieren, ohne vom Benutzer bemerkt zu werden.

Als Riskware zählen auch einige Programme zum automatischen Umschalten der Tastaturbelegung, IRC-Clients, FTP-Server und Dienstprogramme zum Beenden von Prozessen oder zum Verstecken der Arbeit von Prozessen.

1.1.3. Infizierte, verdächtige und potentiell gefährliche Objekte

Der Server, auf dem Anti-Virus installiert ist, enthält eine Auswahl von *Datenbanken*. Die Datenbanken sind Dateien mit Einträgen, mit denen in untersuchten Objekten schädlicher Code von hunderttausenden bekannter Bedrohungen erkannt werden kann. Die Einträge enthalten Informationen über Kontrollbereiche des Codes von Bedrohungen und Algorithmen für die Desinfektion von Objekten, in denen diese Bedrohungen vorkommen.

Wenn Anti-Virus in einem Untersuchungsobjekt Codebereiche findet, die komplett mit den Kontrollbereichen des Codes einer bestimmten Bedrohung in den Datenbankeinträgen übereinstimmen, weist er diesem Objekt den Status *infiziert* zu. Bei teilweiser Übereinstimmung erhält das Objekt (abhängig von bestimmten Bedingungen) den Status *verdächtig*.

Außerdem erkennt Anti-Virus *potentiell gefährliche Objekte*. Dazu wird die heuristische Analyse (Code Analyzer) verwendet. Der Code eines solchen Objekts zeigt in der Regel keine partielle oder komplette Übereinstimmung mit dem Code einer bekannten Bedrohung, enthält aber Befehlsfolgen, die für schädliche Objekte als typisch gelten. Dazu zählen z.B. das Öffnen einer Datei, das Schreiben in eine Datei oder das Abfangen von Interrupt-Vektoren. Die heuristische Analyse ergibt beispielsweise, dass eine Datei aussieht, als sei sie von einem unbekannten Bootvirus infiziert.

Wenn Anti-Virus einem Untersuchungsobjekt den Status infiziert oder verdächtig zuweist, meldet er den Namen der darin gefundenen Bedrohung. Wenn Anti-Virus einem Objekt den Status potentiell gefährlich zuweist, gibt er den Namen der Bedrohung nicht zurück.

Hinweis

Im Dialogfenster zum Anpassen der Sicherheitsparameter und in den Dialogfenstern **Statistik** der Anti-Virus-Konsole wird der Begriff *potentiell gefährliche Objekte* nicht verwendet: Sowohl potentiell gefährliche Objekte als auch tatsächlich verdächtige Objekte (in deren Code Bereiche erkannt wurden, die teilweise mit dem Code bekannter Bedrohungen übereinstimmen) werden als *verdächtig* bezeichnet.

In den übrigen Dialogfenstern der Anti-Virus-Konsole werden die Begriffe *verdächtige Objekte* und *potentiell gefährliche Objekte* unterschieden. Der Begriff *verdächtige Objekte* bezeichnet nur tatsächlich verdächtige Objekte.

1.2. Nach Informationen über Anti-Virus suchen

Auf Fragen zu Auswahl, Kauf, Installation oder Verwendung von Anti-Virus können Sie schnell eine Antwort erhalten.

Kaspersky Lab bietet zu diesem Zweck unterschiedliche Informationsquellen zu dem Programm an, unter denen Sie abhängig von der Dringlichkeit und Bedeutung Ihrer Frage wählen können. Es bestehen folgende Möglichkeiten:

- selbständige Recherche (s. Pkt. 1.2.1 auf S. 20)
- Beratung durch Mitarbeiter der Vertriebsabteilung (s. Pkt. 1.2.2 auf S. 22)
- Beratung durch einen Spezialisten des Technischen Supports, wenn Sie Anti-Virus bereits erworben haben (s. Pkt. 1.2.3 auf S. 22).
- Diskussion Ihrer Frage mit Spezialisten von Kaspersky Lab und anderen Anwendern im Abschnitt des Webforums, das sich mit Anti-Virus befasst (s. Pkt. 1.2.4 auf S. 24).

1.2.1. Selbständige Informationssuche

Sie können folgende Informationsquellen über das Programm verwenden:

- Seite über das Programm auf der Webseite von Kaspersky Lab
- Seite über das Programm auf der Webseite des technischen Supports (in der Wissensdatenbank)
- elektronisches Hilfesystem
- Dokumentation

Seite auf der Webseite von Kaspersky Lab

http://www.kaspersky.com/de/kaspersky_anti-virus_windows_server_enterprise

Auf dieser Seite finden Sie allgemeine Informationen über das Programm, seine Funktionen und Besonderheiten. In unserem Online-Shop können Sie das Programm kaufen oder die Nutzungsdauer verlängern.

Seite auf der Webseite des Technischen Supports (Wissensdatenbank)

http://support.kaspersky.com/de/win_serv_ee_6mp2

Auf dieser Seite finden Sie Artikel, die von Spezialisten des Technischen Supports veröffentlicht wurden.

Diese Artikel bieten nützliche Informationen, Tipps und Antworten auf häufige Fragen zu Kauf, Installation und Verwendung des Programms. Sie sind nach Themen wie "Arbeit mit Lizenzschlüsseln", "Konfiguration des Datenbank-Updates" oder "Beheben von Störungen bei der Arbeit" geordnet. Die Artikel können Fragen behandeln, die nicht nur dieses Programm betreffen, sondern auch andere Produkte von Kaspersky Lab. Außerdem können sie Neuigkeiten über den Technischen Support beinhalten.

Elektronisches Hilfesystem

Zum Lieferumfang des Programms gehört eine Datei mit einem vollständigen Hilfesystem.

Die vollständige Hilfe enthält Informationen darüber, wie der Computerschutz mit Hilfe der Anti-Virus-Konsole in der MMC verwaltet wird: Anzeige des Schutzstatus, Ausführen der Untersuchung unterschiedlicher Computerbereiche, Ausführen anderer Aufgaben. Die Hilfe bietet Informationen über die Steuerung des Programms aus der Befehlzeile, über den Umgang mit den Produktivitäts-Countern von Anti-Virus sowie mit den Countern und Schwachstellen des SNMP-Protokolls.

Um die vollständige Hilfe zu öffnen, wählen Sie auf der Anti-Virus-Konsole im Menü **Hilfe** den Befehl **Hilfe öffnen**.

Sollten Sie Fragen zu einem speziellen Programmfenster haben, dann können Sie die Kontexthilfe verwenden.

Die Kontexthilfe wird im entsprechenden Fenster durch Klick auf die Schaltfläche **Hilfe** oder mit der Taste **<F1>** geöffnet.

Dokumentation

Eine Sammlung von Dokumenten über das Programm enthält umfangreiche Informationen, die für die Arbeit mit dem Programm erforderlich sind. Dazu gehören folgende Dokumente:

- **Typische Verwendungsschemata**. Dieses Dokument erläutert die Einführung von Anti-Virus in Firmennetzwerke.
- **Vergleich mit Kaspersky Anti-Virus 6.0 for Windows Servers**. Dieses Dokument beschreibt die Unterschiede zwischen Anti-Virus und Kaspersky Anti-Virus 6.0 for Windows Servers.
- Die **Installationsanleitung** nennt die Voraussetzungen, die ein Computer für die Installation von Anti-Virus erfüllen muss. Sie enthält eine Anleitung zur Installation und Aktivierung von Anti-Virus. Außerdem werden die Prüfung der Funktionstüchtigkeit und grundlegende Einstellungen erklärt.

- Das **Administratorhandbuch** (vorliegendes Dokument) enthält Informationen über die Arbeit mit der Anti-Virus-Konsole in der MMC, die Verwaltung von Anti-Virus aus der Anwendung Kaspersky Administration Kit und aus der Befehlszeile, den Umgang mit den Produktivitäts-Countern von Anti-Virus sowie mit den Countern und Schwachstellen des SNMP-Protokolls.

Diese Dokumente sind als PDF-Dateien im Lieferumfang von Anti-Virus enthalten.

Außerdem stehen die Dokumente auf der Anti-Virus-Seite der Webseite von Kaspersky Lab zum Download bereit.

Nach der Installation der Anti-Virus-Konsole können Sie das Administratorhandbuch vom **Startmenü** aus öffnen.

1.2.2. Kontakt zur Vertriebsabteilung

Bei Fragen zur Auswahl oder zum Kauf von Anti-Virus sowie zur Verlängerung der Nutzungsdauer stehen Ihnen die Mitarbeiter der Vertriebsabteilung in unserer Zentrale in Moskau unter folgenden Telefonnummern zur Verfügung:

+7 (495) 797-87-00, **+7 (495) 645-79-39**, **+7 (495) 956-70-00**.

Die Beratung kann auf Englisch oder Russisch erfolgen.

Die Mitarbeiter der Vertriebsabteilung beraten Sie auch per E-Mail. Wenden Sie sich an die Adresse sales@kaspersky.com.

Die Vertriebsabteilung berät Sie zu Fragen über die Verwaltung des Schutzes von Firmennetzwerken, die Einführung des Programms in ein Netzwerk und die parallele Verwendung des Programms mit anderen Anwendungen.

1.2.3. Anfrage an den Technischen Support

Nachdem Sie das Programm erworben haben, können Sie von den Spezialisten des Technischen Supports Informationen über das Programm erhalten. Die Beratung erfolgt per Telefon oder über das Internet.

Die Support-Spezialisten beantworten Ihre Fragen zur Installation und Verwendung des Programms und helfen Ihnen dabei, die Folgen von Virenangriffen zu beheben, wenn Ihr Computer infiziert wurde.

Technischer Support am Telefon

Zur Lösung dringender Probleme können Sie den Technischen Support in unserer Moskauer Zentrale unter folgenden Telefonnummern jederzeit direkt erreichen:

+7 (495) 797-87-07, **+7 (495) 645-79-29** oder **+7 (495) 956-87-08**.

Technische Unterstützung für Anwender von Kaspersky-Lab-Programmen wird rund um die Uhr auf Englisch und Russisch angeboten.

Spezialisten für die Anwendung Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition sind an Werktagen zwischen 10:00 und 18:30 Uhr Moskauer Zeit (GMT +3) zu erreichen.

Nennen Sie dem Support-Mitarbeiter den **Aktivierungscode** des Programms oder die **Seriennummer des Schlüssels** (Die Seriennummer wird auf der Anti-Virus-Konsole im Knoten **Schlüssel** in den Eigenschaften des installierten Schlüssels genannt).

E-Mail-Anfrage an den Technischen Support (für registrierte Benutzer)

Sie können Ihre Frage den Spezialisten des Technischen Supports stellen. Füllen Sie dazu das Webformular aus, das sich auf der Seite http://support.kaspersky.com/de/helpdesk.html befindet.

Die Anfrage kann in deutscher, englischer, französischer, spanischer oder russischer Sprache erfolgen.

Um eine E-Mail-Anfrage zu stellen, ist die Angabe der Kundennummer, die Sie bei der Anmeldung auf der Webseite des Technischen Supports erhalten haben, und des Kennworts erforderlich.

Hinweis

Wenn Sie noch nicht als Benutzer eines Kaspersky-Lab-Programms registriert sind, können Sie auf folgender Seite das Anmeldeformular ausfüllen:

https://support.kaspersky.com/de/PersonalCabinet/Registration/Form/

Geben Sie bei der Registrierung den **Aktivierungscode** des Programms oder die **Seriennummer** des Schlüssels an (Die Seriennummer wird auf der Anti-Virus-Konsole im Knoten **Schlüssel** in den Eigenschaften des installierten Schlüssels genannt).

Die Spezialisten des Technischen Supports werden Ihre Frage per E-Mail an die in der Anfrage angegebene Adresse beantworten sowie in Ihrem **Personal Cabinet**

https://support.kaspersky.com/de/PersonalCabinet.

Beschreiben Sie das aufgetretene Problem im Webformular möglichst genau. Machen Sie in den obligatorisch auszufüllenden Feldern folgende Angaben:

- **Typ der Anfrage**. Die Fragen, die häufig von Benutzern gestellt werden, sind in einer Liste vorgegeben. Dazu zählen beispielsweise: "Problem bei der Installation/Deinstallation des Produkts" oder

"Problem bei der Suche/Desinfektion von Viren". Wenn keine der Kategorien zutrifft, wählen Sie den Punkt "Allgemeine Frage".

- **Name des Produkts**: Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition
- **Anfragetext**. Beschreiben Sie das Problem möglichst genau.
- **Kundennummer und Kennwort**. Geben Sie die Kundennummer und das Kennwort an, die sich bei der Anmeldung auf der Webseite des Technischen Supports erhalten haben.
- **E-Mail-Adresse**. An diese Adresse werden die Spezialisten des Technischen Supports Ihre Anfrage beantworten.

1.2.4. Diskussion von Kaspersky-Lab-Programmen im Webforum

Wenn Ihre Frage keine dringende Antwort erfordert, können Sie sie mit den Spezialisten von Kaspersky Lab und mit anderen Anwendern in unserem Forum unter der Adresse http://forum.kaspersky.com/ diskutieren.

Im Forum können Sie bereits veröffentlichte Themen nachlesen, eigene Kommentare verfassen, neue Themen eröffnen und die Hilfefunktion verwenden.

Das Forum eignet sich beispielsweise zur Erörterung verschiedener Einführungsschemata in Firmen und Konfigurationsvarianten für das Programm.

TEIL 1. KONFIGURATION UND VERWALTUNG ÜBER DIE MMC-KONSOLE

Dieser Teil bietet folgende Informationen:

- Start der Anti-Virus-Konsole in der MMC, Zugriff auf Anti-Virus-Funktionen gewähren, Beschreibung des Erscheinungsbilds des Konsolenfensters (s. Kapitel 2 auf S. 26)
- Konfiguration der allgemeinen Anti-Virus-Parameter (s. Kapitel 3 auf S. 43)
- Import und Export von Parametern für Anti-Virus und seiner einzelner Funktionskomponenten (s. Kapitel 4 auf S. 48)
- Begriff einer Aufgabe in Anti-Virus, Aufgabentypen, Operationen mit Aufgaben, Konfiguration eines Aufgabenzeitplans, Anzeige einer Aufgabenstatistik, Start einer Aufgabe mit den Rechten eines anderen Benutzerkontos (s. Kapitel 5 auf S. 52)
- Konfiguration des Echtzeitschutzes für einen Server (s. Kapitel 6 auf S. 68)
- Zugriffssperre von Computern auf den Server bei Ausführung der Aufgabe **Echtzeitschutz für Dateien** (s. Kapitel 7 auf S. 96)
- vertrauenswürdige Zone (s. Kapitel 8 auf S. 109)
- Konfiguration für Virensuche (s. Kapitel 9 auf S. 121)
- Update der Datenbanken und Programm-Module von Anti-Virus (s. Kapitel 10 auf S. 150)
- Quarantäne zur Isolierung von verdächtigen Objekten (s. Kapitel 11 auf S. 170)
- Sicherungskopieren von Dateien vor der Desinfektion oder dem Löschen, Verwendung des Backup-Speichers (s. Kapitel 12 auf S. 189)
- Protokollierung von Ereignissen und Anti-Virus-Statistik (s. Kapitel 13 auf S. 203)
- Installation und Löschen von Schlüsseln (s. Kapitel 14 auf S. 229)
- Konfiguration von Benachrichtigungen (s. Kapitel 15 auf S. 235).

KAPITEL 2. ARBEITEN MIT DER ANTI-VIRUS-KONSOLE IN DER MMC UND ZUGRIFF AUF ANTI-VIRUS-FUNKTIONEN

Dieses Kapitel enthält folgende Informationen:

- Anti-Virus-Konsole in der MMC (s. Pkt. 2.1 auf S. 26)
- zusätzliche Einstellungen nach der Installation der Anti-Virus-Konsole in der MMC auf einem anderen Computer (s. Pkt. 2.2 auf S. 27)
- Start der Anti-Virus-Konsole aus dem **Startmenü** (s. Pkt. 2.3 auf S. 33)
- Funktionen des Anti-Virus-Symbols im Infobereich der Taskleiste des geschützten Servers (s. Pkt. 2.4 auf S. 34)
- Erscheinungsbild des Fensters der Anti-Virus-Konsole (s. Pkt. 2.5 auf S. 36)
- Einschränkung der Zugriffsrechte für die Anti-Virus-Funktionen (s. Pkt. 2.6 auf S. 36)
- Start und Beenden des Anti-Virus-Diensts (s. Pkt. 2.7 auf S. 41).

2.1. Anti-Virus-Konsole in der MMC

Die Anti-Virus-Konsole ist ein eigenständiges Snap-In, das in der MMC-Konsole (Microsoft Management Console) hinzugefügt wird.

Beim Installieren der Anti-Virus-Konsole speichert der Installationsassistent die Datei kavfs.msc im Anti-Virus-Ordner und fügt das Anti-Virus-Snap-In zur Liste der eigenständigen Microsoft Windows-Snap-Ins hinzu.

Sie können die Anti-Virus-Konsole auf dem geschützten Server öffnen, indem Sie sie aus dem **Startmenü** oder aus dem Kontextmenü des Anti-Virus-Symbols im Infobereich der Taskleiste starten.

Sie können die msc-Datei des Anti-Virus-SnapIns starten oder das Anti-Virus-SnapIn in die vorhandene MMC-Konsole als neues Element in deren Baum einfügen. In der 64-Bit-Version von Microsoft Windows können Sie das Anti-Virus-SnapIn nur in die MMC der 32-Bit-Version (MMC32) einfügen: Öffnen Sie die MMC aus der Kommandozeile mit dem Befehl `mmc.exe /32.`

Sie können Anti-Virus über die Konsole in der MMC steuern, die auf dem geschützten Server oder auf einem beliebigen Computer im lokalen Netzwerk installiert ist (s. Pkt. 2.2 auf S. 27).

Einer Konsole, die im Autorenmodus geöffnet ist, können mehrere Anti-Virus-Snap-Ins hinzugefügt werden, um aus dieser Konsole den Schutz mehrerer Server, auf denen Anti-Virus installiert ist, zu verwalten.

2.2. Zusätzliche Einstellungen nach der Installation der Anti-Virus-Konsole in der MMC auf einem anderen Computer

Wenn Sie die Anti-Virus-Konsole nicht auf dem geschützten Server installiert haben, sondern auf einem anderen Computer, führen Sie folgende Aktionen aus, um Anti-Virus auf dem geschützten Server fernzusteuern:

- Fügen Sie auf dem geschützten Server die Anti-Virus-Benutzer zu der Gruppe **KAVWSEE Administrators** hinzu (s. Pkt. 2.2.1 auf S. 28).
- Wenn der geschützte Server unter Microsoft Windows Server 2008 läuft, erlauben Sie auf dem Server Netzwerkverbindungen für die Prozessdatei des Verwaltungsdiensts von Kaspersky Anti-Virus kavfsgt.exe (s. Pkt. 2.2.2 auf S. 29).
- Wenn der Remote-Computer unter Microsoft Windows XP mit Service Pack 1 läuft, deaktivieren Sie auf dem Computer die Windows-Firewall, um die Netzwerkverbindungen für die darauf installierte Anti-Virus-Konsole freizugeben (s. Pkt. 2.2.3 auf S. 30).
- Für die Anti-Virus-Konsole auf einem Computer mit Microsoft Windows XP mit Service Pack 2 oder Microsoft Windows Vista: Wenn Sie bei der Installation der Konsole den Parameter **Netzwerkverbindungen für die Konsole von Kaspersky Anti-Virus erlauben** nicht aktiviert haben, erlauben Sie die Netzwerkverbindungen für die Konsole über die Firewall auf diesem Computer manuell (s. Pkt. 2.2.4 auf S. 31).

2.2.1. Anti-Virus-Benutzer zur Gruppe KAVWSEE Administrators auf dem geschützten Server hinzufügen

Um Anti-Virus über eine Anti-Virus-Konsole in der MMC zu verwalten, die auf einem anderen Computer installiert ist, müssen die Anti-Virus-Benutzer unbeschränkten Zugriff auf den *Verwaltungsdienst von Anti-Virus* (*Kaspersky Anti-Virus Management*) auf dem geschützten Server besitzen. Standardmäßig besitzen die Benutzer, die der Gruppe der lokalen Administratoren angehören, Zugriff auf den Dienst.

Hinweis

Die Dienste, die von Anti-Virus registriert werden, können Sie dem Dokument *Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition. Installationsanleitung* entnehmen.

Sie können folgenden Typen von Benutzerkonten den Zugriff auf den Verwaltungsdienst von Anti-Virus gewähren:

- **Lokales Benutzerkonto** des Computers, auf dem die Anti-Virus-Konsole installiert ist. Um eine Verbindung herzustellen, muss auf dem geschützten Server ein lokales Benutzerkonto mit den gleichen Daten registriert sein.
- **Benutzerkonto, das in der Domäne registriert ist**, in der der Computer mit der installierten Anti-Virus-Konsole registriert ist. Um eine Verbindung herzustellen, muss der geschützte Server entweder in der gleichen Domäne oder in einer Domäne, die für diese Domäne als vertrauenswürdig gilt, registriert sein.

Während der Installation meldet Anti-Virus auf dem geschützten Server die Gruppe **KAVWSEE Administrators** an. Für die Benutzer dieser Gruppe ist der Zugriff auf den Verwaltungsdienst von Anti-Virus erlaubt. Sie können den Zugriff auf den Verwaltungsdienst von Anti-Virus für Benutzer erlauben oder sperren, indem Sie die Benutzer zur Gruppe **KAVWSEE Administrators** hinzufügen oder aus der Gruppe entfernen.

Um den Zugriff auf den Verwaltungsdienst von Anti-Virus zu erlauben oder zu verbieten:

1. Wählen Sie auf dem geschützten Server **Start** → **Einstellungen** → **Systemsteuerung**. Wählen Sie im Fenster **Systemsteuerung** den Punkt **Verwaltung** → **Computerverwaltung**.

2. Öffnen Sie in der Konsolenstruktur **Computerverwaltung** zuerst den Knoten **Lokale Benutzer und Gruppen** und anschließend den Knoten **Gruppen**.

3. Doppelklicken Sie auf die Gruppe **KAVWSEE Administrators** und führen Sie im Dialogfenster **Eigenschaften** folgende Aktionen aus:

   - Um die Fernverwaltung von Anti-Virus mit Hilfe der Anti-Virus-Konsole für einen Benutzer zu erlauben, fügen Sie ihn zur Gruppe **KAVWSEE Administrators** hinzu.

   - Um die Fernverwaltung von Anti-Virus mit Hilfe der Anti-Virus-Konsole für einen Benutzer zu verbieten, entfernen Sie ihn aus der Gruppe **KAVWSEE Administrators**.

4. Klicken Sie im Dialogfenster **Eigenschaften** auf die Schaltfläche **OK**.

2.2.2. Auf einem Server mit Microsoft Windows Server 2008 Netzwerkverbindungen für den Verwaltungsdienst von Kaspersky Anti-Virus erlauben

Um eine Verbindung zwischen der Konsole und dem Anti-Virus-Verwaltungsdienst herzustellen, müssen Sie die Netzwerkverbindungen für den Verwaltungsdienst von Kaspersky Anti-Virus auf dem geschützten Server über die Firewall erlauben.

Um die Netzwerkverbindungen für den Verwaltungsdienst von Kaspersky Anti-Virus zu erlauben:

1. Wählen Sie auf dem geschützten Server mit dem Betriebssystem Microsoft Windows Server 2008 **Start** → **Systemsteuerung** → **Sicherheit** → **Windows-Firewall**.

2. Klicken Sie im Fenster **Eigenschaften der Windows-Firewall** auf **Eigenschaften ändern**.

3. Aktivieren Sie auf der Registerkarte **Ausnahmen** in der Liste mit den vordefinierten Ausnahmen die Kontrollkästchen **COM + Netzwerkzugriff**, **Windows Management Instrumentation (WMI)** und **Remote Administration**.

4. Klicken Sie auf die Schaltfläche **Programm hinzufügen**.

5. Geben Sie im Dialogfenster **Programm hinzufügen** die Datei kavfsgt.exe an. Sie befindet sich im Ordner, den Sie bei der Installation der Anti-Virus-Konsole in der MMC als Zielordner angegeben haben. Der vollständige Pfad der Datei lautet standardmäßig:
   - für die *32-Bit-Version von Microsoft Windows*: %ProgramFiles%\Kaspersky Lab\Kaspersky Anti-Virus 6.0 For Windows Servers Enterprise Edition\kavfsgt.exe
   - für die *64-Bit-Version von Microsoft Windows*: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Anti-Virus 6.0 For Windows Servers Enterprise Edition\kavfsgt.exe.
6. Klicken Sie auf die Schaltfläche **OK**.
7. Klicken Sie im Dialogfenster **Eigenschaften der Windows-Firewall** auf **OK**.

2.2.3. Netzwerkverbindungen für die Anti-Virus-Konsole in der MMC unter Microsoft Windows XP mit Service Pack 1 erlauben

Wenn die Anti-Virus-Konsole auf einem Computer mit dem Betriebssystem Microsoft Windows XP Service Pack 1 installiert ist, muss die Windows-Firewall auf diesem Computer deaktiviert werden, um die Netzwerkverbindungen für die Konsole zu erlauben:

1. Wählen Sie auf dem Computer, auf dem die Anti-Virus-Konsole in der MMC installiert ist, den Punkt **Start** → **Systemsteuerung** → **Netzwerkverbindungen**.
2. Öffnen Sie das Kontextmenü auf dem Namen einer Netzwerkverbindung (zum Beispiel **Local Area Connection**) und wählen Sie den Befehl **Eigenschaften**.
3. Deaktivieren Sie im Dialogfenster **Eigenschaften von <Name der Netzwerkverbindung>** auf der Registerkarte **Erweitert** das Kontrollkästchen **Meine Internetverbindung schützen**.
4. Klicken Sie auf **OK**.

2.2.4. Netzwerkverbindungen für die Anti-Virus-Konsole in der MMC unter Microsoft Windows XP mit Service Pack 2 oder Microsoft Windows Vista erlauben

Die Anti-Virus-MMC-Konsole auf dem Remote-Computer verwendet das Protokoll DCOM, um Informationen über Anti-Virus-Ereignisse (untersuchte Objekte, abgeschlossene Aufgaben usw.) vom Anti-Virus-Verwaltungsdienst auf dem geschützten Server zu erhalten.

Wenn die Anti-Virus-Konsole auf einem Computer mit dem Betriebssystem *Microsoft Windows XP Service Pack 2 oder Microsoft Windows Vista* installiert ist, müssen auf diesem Computer in der Firewall die Netzwerkverbindungen erlaubt werden, um die Verbindung zwischen Konsole und Anti-Virus-Verwaltungsdienst herzustellen.

Gehen Sie folgendermaßen vor:

- Vergewissern Sie sich, dass der anonyme Remote-Zugriff auf COM-Anwendungen erlaubt ist (nicht aber der Remote-Start und die Remote-Aktivierung von COM-Anwendungen) und
- schalten Sie in der Windows-Firewall den TCP-Port 135 frei und erlauben Sie Netzwerkverbindungen für die ausführbare Prozessdatei des Anti-Virus-Verwaltungsdiensts kavfsrcn.exe.

  Über TCP-Port 135 greift der Client-Computer, auf dem die Anti-Virus-MMC-Konsole installiert ist, auf den geschützten Server zu und der Server beantwortet seine Anfragen.

Um den anonymen Fernzugriff auf COM-Anwendungen zu erlauben:

1. Öffnen Sie auf dem Computer, auf dem die Anti-Virus-Konsole in der MMC installiert ist, die Konsole **Komponentendienste**: Wählen Sie den Punkt **Start** → **Ausführen**, geben Sie **dcomcnfg** ein und klicken Sie auf **OK**.
2. Öffnen Sie in der Konsole **Komponentendienste** des Computers den Knoten **Computer**, öffnen Sie das Kontextmenü auf dem Knoten **Arbeitsplatz** und wählen Sie den Befehl **Eigenschaften**.
3. Klicken Sie im Dialogfenster **Eigenschaften** auf der Registerkarte **COM-Sicherheit** in der Parametergruppe **Zugriffsberechtigungen** auf die Schaltfläche **Limits bearbeiten**.

4. Vergewissern Sie sich im Dialogfenster **Zugriffsberechtigungen**, dass für den Benutzer **ANONIMOUS LOGON** das Kontrollkästchen **Remotezugriff** aktiviert ist.

5. Klicken Sie auf **OK**.

Um in der Windows-Firewall den TCP-Port 135 freizuschalten und Netzwerkverbindungen für die ausführende Prozessdatei des Anti-Virus-Vervaltungsdiensts zu erlauben:

1. Schließen Sie auf dem Remote-Computer die Anti-Virus-Konsole in der MMC.

2. Führen Sie eine der folgenden Aktionen aus:

   - Wählen Sie in *Microsoft Windows XP mit Service Pack 2 oder höher* den Punkt **Start** → **Systemsteuerung** → **Windows-Firewall**.

   - Wählen Sie in *Microsoft Windows Vista* den Punkt **Start** → **Systemsteuerung** → **Windows-Firewall** und klicken Sie im Fenster **Windows-Firewall** auf **Eigenschaften ändern.**

3. Klicken Sie im Dialogfenster **Windows-Firewall** (**Eigenschaften der Windows-Firewall**) auf der Registerkarte **Ausnahmen** auf die Schaltfläche **Port hinzufügen**.

4. Geben Sie im Feld **Name** geben Sie den Namen des Ports an **RPC(TCP/135)** oder geben Sie einen anderen Namen an, z. B. **DCOM für Antivirus**. Geben Sie im Feld **Portnummer** die Portnummer an: **135**.

5. Wählen Sie das Protokoll **TCP**.

6. Klicken Sie auf **OK**.

7. Klicken Sie auf der Registerkarte **Ausnahmen** auf die Schaltfläche **Programm hinzufügen**.

8. Geben Sie im Dialogfenster **Programm hinzufügen** die Datei kavfsrcn.exe an. Sie befindet sich in dem Ordner, den Sie bei der Installation der Anti-Virus-Konsole in der MMC als Zielordner angegeben haben. Der vollständige Pfad lautet standardmäßig:

   - für die *32-Bit-Version von Microsoft Windows*: %ProgramFiles%\Kaspersky Lab\Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition Admins Tools\kavfsrcn.exe.

   - für die *64-Bit-Version von Microsoft Windows*: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition Admins Tools\kavfsrcn.exe.

9. Klicken Sie auf **OK**.

10. Klicken Sie im Dialogfenster **Windows-Firewall** (**Eigenschaften der Windows-Firewall**) auf **OK**.

> **Hinweis**
>
> *Um die neuen Verbindungsparameter zu übernehmen:* Wenn die Anti-Virus-Konsole geöffnet war, während Sie die Verbindung zwischen dem geschützten Server und dem Computer, auf dem die Konsole installiert ist, angepasst haben, schließen Sie die Konsole, warten Sie 30-60 Sekunden (bis der Prozess zur Remote-Verwaltung von Anti-Virus kavfsrcn.exe beendet wurde) und starten Sie anschließend die Konsole neu.

2.3. Start der Anti-Virus-Konsole aus dem *Startmenü*

Überzeugen Sie sich davon, dass die Anti-Virus-Konsole auf dem Computer installiert ist.

Um die Anti-Virus-Konsole aus dem ***Startmenü*** *zu starten:*

1. Gehen Sie nacheinander auf **Start** → **Programme** → **Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition** → **Konsole von Kaspersky Anti-Virus**.

> **Anmerkung**
>
> Wenn Sie vorhaben zur Anti-Virus-Konsole andere Snap-Ins zur Anti-Virus-Konsole hinzuzufügen, öffnen Sie die Konsole im **Autorenmodus**: wählen Sie **Start** → **Programme** → **Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition** → **Administration**, öffnen Sie das Kontextmenü in der Anwendung **Kaspersky Anti-Virus-Konsole** und wählen Sie **Autor**.

Wenn Sie die Anti-Virus-Konsole auf dem geschützten Server gestartet haben, öffnet sich das Konsolenfenster (s. Abbildung 1).

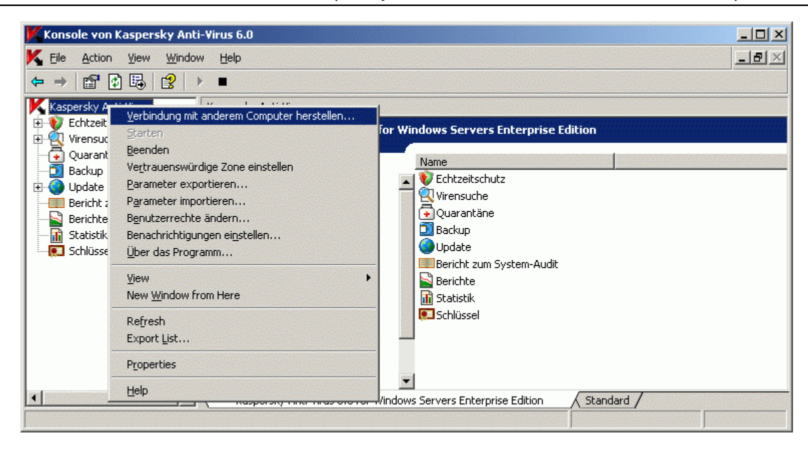


Abbildung 1. Fenster der Anti-Virus-Konsole

2. Wenn Sie die Anti-Virus-Konsole nicht auf dem geschützten Server gestartet haben, sondern auf einem anderen Computer, stellen Sie eine Verbindung mit dem Server her, den Sie administrieren wollen: öffnen Sie das Kontextmenü auf dem Namen des Anti-Virus Snap-In, wählen Sie das Befehl **Verbindung mit anderen Computer herstellen**, danach in dem Dialogfenster **Computer wählen** wählen Sie **Anderer Computer** und geben Sie den Netzwerknamen des geschützten Server.

   Wenn das Benutzerkonto, mit dem Sie sich bei Microsoft Windows anmelden, nicht die Berechtigungen für den Verwaltungsdienst des Anti-Virus am Server hat, können Sie ein anderes Benutzerkonto angeben, das diese Rechte hat. Details dazu, mit welchen Benutzerkonten Sie auf den Verwaltungsdienst des Anti-Virus zugreifen können, lesen Sie in Pkt. 2.2.1 auf S. 28.

2.4. Anti-Virus-Symbol im Infobereich der Taskleiste

Jedes Mal, wenn Anti-Virus nach dem Neustart des Servers automatisch gestartet wird, erscheint im Infobereich der Taskleiste das Anti-Virus-Symbol. Es wird standardmäßig angezeigt, wenn Sie bei der Installation des Anti-Virus als zu installierende Komponenten die Komponente **Taskleistenanwendung** angeklickt haben.

Das Anti-Virus-Symbol kann die folgenden Zustände annehmen:

Es ist farbig (aktiv), wenn zurzeit die eine der Aufgaben ausgeführt werden: **Echtzeitschutz für Dateien** und **Skript-Untersuchung** (Details zu den Aufgaben des Echtzeitschutzes finden Sie in Pkt. 6.1 auf S. 68).

Es ist schwarzweiß (inaktiv), wenn zurzeit die Aufgaben **Echtzeitschutz für Dateien** und **Skript-Untersuchung** nicht ausgeführt werden.

Mit einem Klick der rechten Maustaste auf das Anti-Virus-Symbol öffnen Sie das Kontextmenü, das in der Abbildung 2 dargestellt ist.

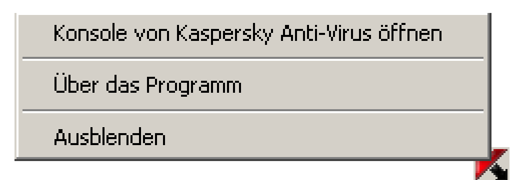


Abbildung 2. Kontextmenü des Anti-Virus-Symbols

Das Kontextmenü hat die folgenden Einträge:

Befehl	**Beschreibung**
Konsole von Kaspersky Anti-Virus öffnen	Der Befehl öffnet die Anti-Virus-Konsole in der MMC (falls installiert).
Über das Programm	Dieser Befehl öffnet das Fenster **Über das Programm** mit Informationen zu Anti-Virus. Wenn Sie als Benutzer von Anti-Virus registriert sind, enthält das Fenster **Über das Programm** Informationen über installierte dringende Updates.
Ausblenden	Der Befehl sorgt dafür, dass das Anti-Virus-Symbol nicht mehr in der Taskleiste angezeigt wird. Um das Anti-Virus-Symbol anzuzeigen, gehen Sie im **Startmenü**, dann auf **Programme**→ **Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition** → **Taskleistenanwendung**.

In den Einstellungen der allgemeinen Anti-Virus-Parameter können Sie festlegen, ob das Anti-Virus-Symbol angezeigt werden soll, wenn Anti-Virus nach dem Neustart des Servers automatisch gestartet wird (s. Pkt. 3.2 auf S. 43).

2.5. Fenster der Anti-Virus-Konsole

Das Fenster Anti-Virus-Konsole (s. Abbildung 3) besteht aus dem Konsolenfenster und dem Ergebnisfenster. In der Konsolenstruktur stehen die Knoten der Funktionalkomponenten des Anti-Virus und im Ergebnisfenster stehen Informationen über den in der Konsolenstruktur ausgewählten Knoten.

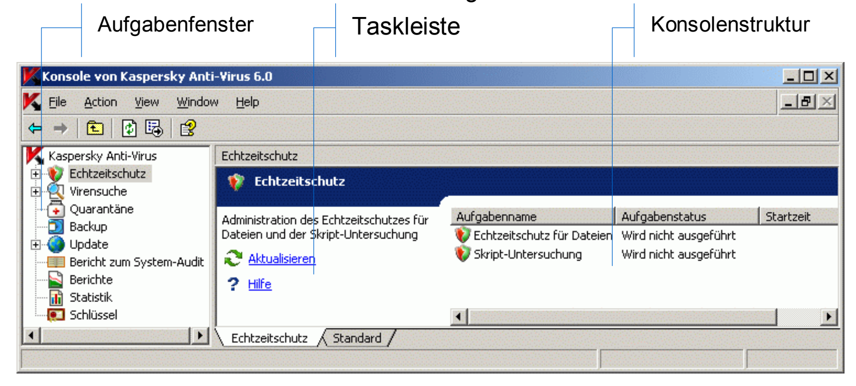


Abbildung 3. Anti-Virus-Konsole

Die Anti-Virus-Konsole enthält daneben noch den Aufgabenbereich, wenn Sie sie aus dem **Startmenü** starten (aus msc-Datei, die bei Installation des Anti-Virus gespeichert wird). Wenn Sie das Anti-Virus-Snap-In in die vorhandene MMC-Konsole eingefügt haben, enthält die Konsole nicht den Aufgabenbereich.

2.6. Abgrenzung der Zugangsrechte für die Funktionen des Anti-Virus

In diesem Abschnitt stehen die folgenden Informationen:

- Zugangsrechte für die Anti-Virus-Funktionen (s. Pkt. 2.6.1 auf S. 37)
- Gewährung von Zugangsrechten für die Anti-Virus-Funktionen (s. Pkt. 2.6.2 auf S. 39)

2.6.1. Zugangsrechte für die Funktionen des Anti-Virus

Standardmäßig haben die Benutzer der Gruppe **Lokale Administratoren** und Benutzer der Gruppe **KAVWSEE Administrators**, welche auf dem geschützten Server erstellt wurde, den Zugriff auf alle Funktionen des Anti-Virus.

Die Benutzer, die auf die Anti-Virus-Funktionen **Verwaltung der Benutzerrechte** zugreifen können, dürfen den Zugriff auf die Anti-Virus-Funktionen an andere Benutzer vergeben, die am geschützten Server angemeldet sind oder zur Domäne gehören.

Wenn ein Benutzer in der Benutzerliste des Anti-Virus nicht eingetragen ist, kann er die Anti-Virus-Konsole nicht sehen.

Sie können an Benutzer (an eine Gruppe der Benutzer) die folgenden Zugangsrechte vergeben:

- für alle Funktionen des Anti-Virus (**Komplettzugriff**)
- für alle Funktionen des Anti-Virus, außer Verwaltung der Benutzerrechte (**Änderung**)
- Anzeige der funktionellen Komponente des Anti-Virus, allgemeine Parameter des Anti-Virus, Funktionen- und Aufgabenparameter, Statistik und Benutzerrechte (**Lesen**).

Außerdem können Sie erweiterte Einstellungen bei den Zugriffsrechten vornehmen: Zugang zu einzelnen Funktionen des Anti-Virus gestatten oder unterbinden. Die Funktionen, deren Zugriff Sie verwalten können, stehen in der folgenden Tabelle 1.

Tabelle 1. Abgrenzung der Zugangsrechte für die Funktionen des Anti-Virus

Funktion	Beschreibung
Lesen der Statistik	Anzeige der Anti-Virus-Aufgaben, der Statistik für die Funktionalkomponenten des Anti-Virus und der Statistik für ausführende Aufgaben
Verwaltung des Aufgabenstatus	Starten / Beenden / Anhalten / Wiederaufnahme von Anti-Virus-Aufgaben
Aufgabenverwaltung	Erstellen und Löschen von Aufgaben des Virensuche

Funktion	Beschreibung
Lesen von Parametern	• Anzeige von allgemeinen Anti-Virus-Parametern und Aufgabenparametern • Anzeige von Parametern für Berichte, Benachrichtigungen und Bericht zum System-Audit • Export von Anti-Virus-Parametern
Änderung von Parametern	• Anzeigen und Bearbeiten von Anti-Virus-Parametern • Import und Export von Anti-Virus-Parametern • Anzeigen und Bearbeiten von Aufgabenparametern • Anzeigen und Bearbeiten von Parametern für Berichte, Benachrichtigungen und Bericht zum System-Audit
Verwalten von Quarantäne und Backup	• Verschieben von Objekten in die Quarantäne • Löschen von Objekten aus der Quarantäne und von Dateien aus dem Backup • Wiederherstellen von Objekten aus dem Backup und aus der Quarantäne
Lesen von Berichten	Anzeigen von allgemeinen und detaillierten Berichten zur Aufgabenausführung im Knoten **Berichte** und von Ereignissen im Knoten **Bericht zum System-Audit**
Verwaltung von Berichten	Löschen von Objekten und Leeren des Berichts zum System-Audit
Verwaltung der Schlüssel	Aktivierung und Deaktivierung von Schlüsseln
Lesen von Benutzerrechte	Anzeige der Benutzerliste des Anti-Virus
Verwaltung von Benutzerrechten	• Hinzufügen und Löschen von Anti-Virus-Benutzern • Änderung der Benutzer-Zugangsrechte für die Funktionen des Anti-Virus

2.6.2. Einstellen der Zugangsrechte für die Funktionen des Anti-Virus

Um einen Benutzer (eine Gruppe) hinzuzufügen oder zu löschen oder die Zugangsrechte eines Benutzers (einer Gruppe) zu ändern, machen Sie Folgendes:

1. Öffnen Sie in der Konsolenstruktur das Kontextmenü mit einem Rechtsklick auf das Anti-Virus-Snap-In und gehen Sie auf **Benutzerrechte ändern**.

   Es öffnet sich das Dialogfenster **Berechtigungen** (s. Abbildung 4).

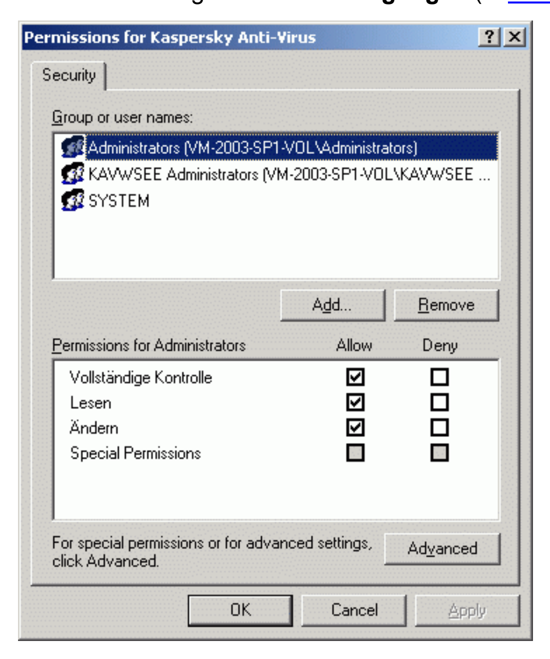


Abbildung 4. Dialogfenster **Berechtigungen**

2. Im Dialogfenster **Berechtigungen** führen Sie folgende Aktionen durch:

   - Um einen Benutzer (eine Gruppe) in die Benutzerliste des Anti-Virus einzufügen, klicken Sie auf die Schaltfläche **Hinzufügen** und wählen Sie die Benutzer oder die Gruppen aus, die Sie hinzufügen wollen.

   - Um an einen hinzugefügten Benutzer (einer Gruppe) Zugangsrechte für die Anti-Virus-Funktionen zu vergeben, wählen Sie den Be-

nutzer (die Gruppe) unter der Überschrift **Gruppen- oder Benutzernamen** und unter der Überschrift **Berechtigungen für <Benutzer (Gruppe)>** setzen Sie das Häkchen im Kontrollkästchen **Zulassen** für die folgenden Zugangsrechte:

  - **Vollständige Kontrolle**, um den Zugriff auf alle Funktionen des Anti-Virus zu gewähren
  - **Lesen**, um den Zugriff auf die Funktionen **Lesen der Statistik**, **Lesen von Parametern**, **Lesen von Berichten** und **Lesen von Benutzerrechten** zu gewähren
  - **Ändern**, um den Zugriff auf alle Funktionen des Anti-Virus zu gewähren, außer der Funktion **Ändern der Benutzerrechte**

- Um in den Modus mit den erweiterten Einstellungen der Benutzerrechte zu wechseln, klicken Sie auf **Erweitert**, im Dialogfenster **Erweiterte Parameter für Sicherheit** markieren Sie den gewünschten Benutzer oder die gewünschte Gruppe und klicken Sie auf die Schaltfläche **Ändern** und setzen Sie im Dialogfenster **Berechtigungseintrag** (s. Abbildung 5) das Häkchen im Kontrollkästchen **Zulassen** oder **Verweigern** neben der Bezeichnung der Funktionen, deren Zugang Sie gestatten oder unterdrücken wollen (Funktionsliste und Kurzbeschreibung stehen in der Tabelle 1). Klicken Sie auf die Schaltfläche **OK**.

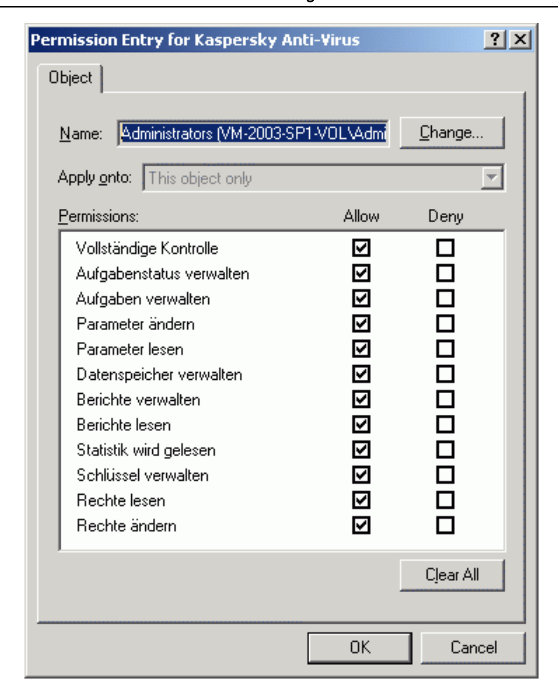


Abbildung 5. Dialogfenster **Berechtigungseintrag**

3. Klicken Sie im Dialogfenster **Berechtigungen** auf die Schaltfläche **OK**.

2.7. Anti-Virus-Dienste starten und anhalten

Standardmäßig wird der Anti-Virus-Dienst automatisch beim Hochfahren des Betriebssystems gestartet. Dieser Dienst regelt die Arbeitsprozesse, die die Aufgaben Echtzeitschutz, Virensuche und Update bedienen.

Standardmäßig werden beim Start des Anti-Virus-Dienst die Aufgaben **Echtzeitschutz für Dateien**, **Skript-Untersuchung, Untersuchung bei Systemstart** und **Integritätskontrolle für Anwendungen** wie auch andere Aufgaben gestartet, die in dem Zeitplan den Eintrag der Starthäufigkeit **Bei Programmstart** zu stehen haben.

Wenn Sie den Anti-Virus-Dienst beenden, werden alle Aufgaben unterbrochen. Nach dem Neustarten des Anti-Virus-Dienstes werden sie nicht automatisch neu

gestartet. Es werden nur solche Aufgaben neu gestartet, die in dem Zeitplan die Starthäufigkeit **Bei Programmstart** zu stehen haben.

Anmerkung

Sie können den Anti-Virus-Dienst nur dann starten und beenden, wenn Sie zur Gruppe der lokalen Administratoren auf dem geschützten Server gehören.

Um den Anti-Virus-Dienst zu beenden bzw. zu starten, öffnen Sie in der Konsolenstruktur das Kontextmenü des Anti-Virus-Snap-Ins und gehen Sie auf einen der folgenden Einträge:

- **Beenden**, um den Anti-Virus-Dienst zu beenden
- **Starten**, um den Anti-Virus-Dienst zu starten.

Außerdem können Sie den Anti-Virus-Dienst über das Snap-In **Dienste** in Microsoft Windows starten und beenden.

KAPITEL 3. ALLGEMEINE ANTI-VIRUS-PARAMETER

In diesem Kapitel stehen die folgenden Informationen:

- Allgemeine Anti-Virus-Parameter (s. Pkt. 3.1 auf S. 43)
- Einstellen der allgemeinen Anti-Virus-Parameter (s. Pkt. 3.2 auf S. 43)

Die allgemeinen Anti-Virus-Parameter werden in Pkt. B.1 auf S. 375 näher beschrieben.

3.1 Allgemeine Anti-Virus-Parameter

Die allgemeinen Anti-Virus-Parameter legen die generellen Bedingungen für die Arbeit von Anti-Virus fest. Dazu gehören folgende Einstellungen: Anzahl der aktiven Prozesse, die von Anti-Virus verwendet werden; Wiederherstellung von Anti-Virus-Aufgaben nach dem Absturz von Aufgaben; Führen eines Berichts zur Ablaufverfolgung; Anlegen von Speicher-Dumps für Anti-Virus-Prozesse bei deren Absturz; Anzeige des Anti-Virus-Symbol, wenn Anti-Virus nach dem Neustart des Servers automatisch gestartet wird; usw.

3.2 Einstellen der allgemeinen Anti-Virus-Parameter

In diesem Abschnitt stehen Informationen darüber, wie die Anti-Virus-Parameter eingestellt werden. Die allgemeinen Parameter werden in Pkt. B.1 auf S. 375 näher beschrieben.

Um die Anti-Virusparameter einzustellen, machen Sie Folgendes:

1. Öffnen Sie in der Konsolenstruktur das Kontextmenü des Anti-Virus-Snap-Ins und gehen Sie auf **Eigenschaften**.
2. Auf den folgenden Registerkarten ändern Sie die Werte der allgemeinen Anti-Virus-Parameter je nach Ihren Wünschen.
   - Auf der Registerkarte **Allgemein** (s. Abbildung 6):

- Tragen Sie die maximale Anzahl der Arbeitsprozesse ein, die vom Anti-Virus gestartet werden können (s. Pkt. B.1.1 auf S. 376)
- Stellen Sie die fixe Anzahl der Prozesse für Aufgaben des Echtzeitschutzes ein (s. Pkt. B.1.2 auf S. 377).
- Stellen Sie die Anzahl der Arbeitsprozesse für Aufgaben zur Virensuche im Hintergrund ein (s. Pkt. B.1.3 auf S. 378).
- Geben Sie die Anzahl der Versuche zur Wiederherstellung von Aufgaben nach einem Absturz von Aufgaben an (s. Pkt. B.1.4 auf S. 379) ein.

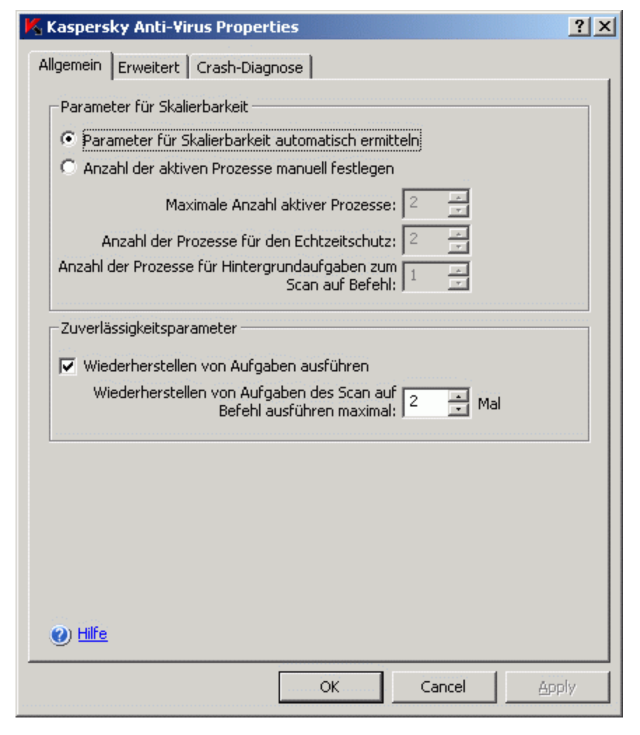


Abbildung 6. Dialogfenster **Eigenschaften: Kaspersky Anti-Virus**, Registerkarte **Allgemein**

- Auf der Registerkarte **Erweitert** (s. Abbildung 7):
  - Legen Sie fest, ob das Anti-Virus-Symbol im Infobereich der Taskleiste des Servers jedes Mal angezeigt werden soll, wenn Anti-Virus nach dem Neustart des Servers automatisch gestar-

tet wird (Details über das Anti-Virus-Symbol s. Pkt. 2.4 auf S. 34).

- Geben Sie an, wie viel Tage Summe- und Detailberichte über die Aufgabenausführung gespeichert werden sollen, die im Knoten **Speichern von Berichten** der Anti-Virus-Konsole dargestellt werden (s. Pkt. B.1.5 auf S. 380).
- Geben Sie an, wie lange soll die Information in den Knoten **Speichern des Berichts zum System-Audit** vorgehalten werden (s. Pkt. B.1.6 auf S. 380).
- Geben Sie die Aktionen des Anti-Virus beim Betrieb mit einer unterbrechungsfreien Stromversorgung an (s. Pkt. B.1.7 auf S. 381).
- Setzen Sie einen Grenzwert für die Anzahl der Tage, nach deren Ablauf die Ereignisse *Datenbanken veraltet*, *Datenbanken stark veraltet* und *Vollständige Untersuchung des Computers lag lange zurück* eintreten werden (s. Pkt. B.1.8 auf S. 382).

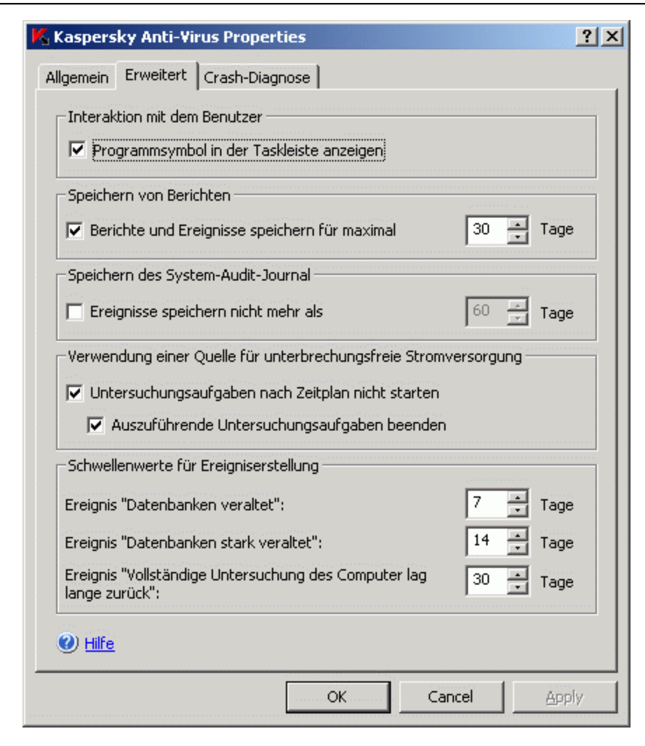


Abbildung 7. Dialogfenster **Eigenschaften: Kaspersky Anti-Virus**, Registerkarte **Erweitert**

- Auf der Registerkarte **Crash-Diagnose** (s. Abbildung 8):
    - Aktivieren oder deaktivieren Sie das Protokoll der Ablaufverfolgung. Bei Bedarf stellen Sie die Protokollparameter ein (s. Pkt. B.1.9 auf S. 382).
    - Aktivieren oder deaktivieren Sie die Dump-Dateien für Anti-Virus-Prozesse (s. Pkt. B.1.10 auf S. 388).

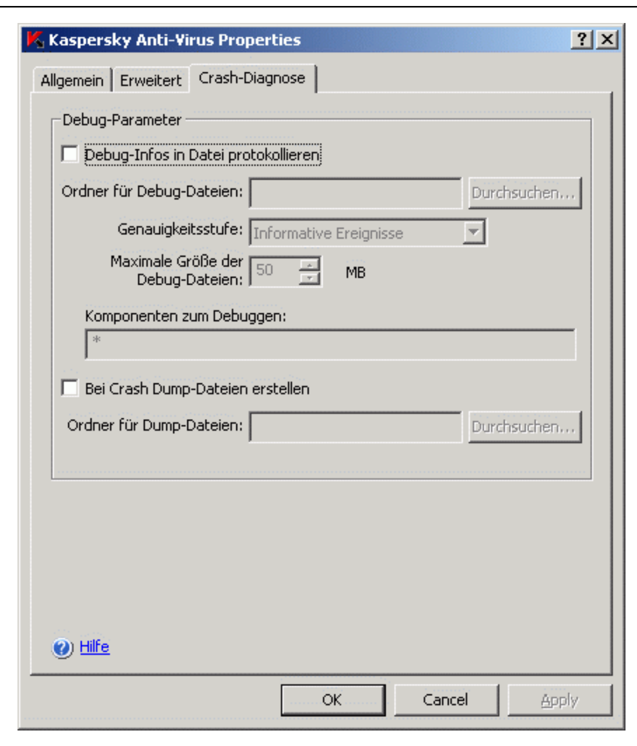


Abbildung 8. Dialogfenster **Eigenschaften: Kaspersky Anti-Virus**, Registerkarte **Crash-Diagnose**

3. Nach dem Sie die Werte der gewünschten allgemeine Anti-Virus-Parameter geändert haben, klicken Sie auf die Schaltfläche **OK**.

KAPITEL 4. IMPORT UND EXPORT VON ANTI-VIRUS-PARAMETERN

In diesem Kapitel stehen die folgenden Informationen:

- Import und Export der Parameter (s. Pkt. 4.1 auf S. 48)
- Export der Parameter (s. Pkt. 4.2 auf S. 49)
- Import der Parameter (s. Pkt. 4.3 auf S. 50)

4.1. Im- und Export der Parametern

Wenn Sie einheitliche Parameterwerte des Anti-Virus für mehrere geschützte Server setzen müssen, können Sie die Anti-Virus-Parameter auf einem Server einstellen, sie in eine Konfigurationsdatei mit dem XML-Format exportieren und dann aus dieser Datei auf den anderen Server in den Anti-Virus importieren.

Sie können in einer Konfigurationsdatei alle Anti-Virus-Parameter oder Parameter der ausgewählten Funktionalkomponenten speichern.

Wenn Sie alle Anti-Virus-Parameter exportieren, speichert Anti-Virus in der Datei die allgemeinen Anti-Virus-Parameter und die Parameter der folgenden Funktionalkomponenten:

- Echtzeitschutz für Dateien
- Skript-Untersuchung
- Zugriff von Computern sperren
- Virensuche
- Update der Anti-Virus-Datenbanken und -Module
- Quarantäne
- Backup
- Berichte
- Benachrichtigungen
- Vertrauenswürdige Zone

und er speichert die Berechtigungen der Benutzerkonten.

Anti-Virus exportiert die Parameter von Gruppenaufgaben, die Sperrliste für den Zugriff von Computern nicht.

Alle von Anti-Virus verwendeten Kennwörter, wie beispielsweise Daten von Benutzerkonten für den Start von Aufgaben oder für die Verbindung mit einem Proxyserver, werden vor dem Export in verschlüsselter Form in der Konfigurationsdatei gespeichert. Die Kennwörter können aber von Anti-Virus nur auf den gleichen Computer importiert werden, wenn Anti-Virus nicht neu installiert oder aktualisiert wurde. Die Kennwörter können von Anti-Virus nicht auf einen anderen Computer importiert werden. Nach dem Import von Parametern auf einen anderen Computer müssen alle Kennwörter manuell eingegeben werden.

Wenn zum Zeitpunkt des Exports von Parametern eine Richtlinie des Programms Kaspersky Administration Kit gültig ist, exportiert Anti-Virus nicht die aus der Richtlinie übernommenen Werte, sondern die Werte, die vor dem Übernehmen galten.

Anmerkung

Zu importierende Aufgabenparameter werden nicht für zurzeit ausgeführte Aufgaben übernommen. Sie gelten nach einem Neustart der Aufgabe. Es wird empfohlen, die Aufgaben der Funktionalkomponenten vor dem Parameter-Import zu beenden.

4.2. Export der Parameter

Um die Parameter in eine Konfigurationsdatei zu exportieren, machen Sie Folgendes:

1. Wenn Sie die Parameter auf der Anti-Virus-Konsole geändert haben, klicken Sie vor dem Export der Parameter auf die Schaltfläche **Speichern**, um die neuen Werte zu speichern.

2. Führen Sie eine der folgenden Aktionen durch:

   - Um alle Parameter des Anti-Virus zu exportieren, öffnen Sie in der Konsolenstruktur das Kontextmenü mit einem Rechtsklicke auf den Namen des Anti-Virus-Snap-Ins und gehen Sie auf **Parameter exportieren**.

   - Um die Parameter einer einzelnen Funktionalkomponente zu exportieren, öffnen Sie in der Konsolenstruktur das Kontextmenü des Knotens dieser Funktionalkomponente und gehen Sie auf **Parameter exportieren**.

Darauf öffnet sich das Begrüßungsfenster des Assistenten für den Parameter-Export.

3. Folgen Sie den Anweisungen in den Fenstern des Assistenten: Geben Sie einen Namen für die Konfigurationsdatei an, in die Sie die Parameter speichern wollen, weiterhin noch den Pfad.

   Wenn Sie den Pfad angeben, können Sie die Umgebungsvariablen des Systems verwenden. Dagegen können Sie die benutzerdefinierten Umgebungsvariablen nicht verwenden.

   Hinweis

   Wenn zum Zeitpunkt des Exports von Parametern eine Richtlinie des Programms Kaspersky Administration Kit gültig ist, exportiert Anti-Virus nicht die aus der Richtlinie übernommenen Werte, sondern die Werte, die vor dem Übernehmen galten.

4. Klicken Sie im Fenster **Die Anwendungsparameter sind exportiert worden** auf **OK**, um den Assistenten zum Parameter-Export zu schließen.

4.3. Import der Parameter

Um die Parameter aus einer Konfigurationsdatei zu importieren, machen Sie Folgendes:

1. Führen Sie eine der Aktionen durch:

   - Um alle Parameter des Anti-Virus zu importieren, öffnen Sie in der Konsolenstruktur das Kontextmenü mit dem Namen des Anti-Virus-Snap-Ins und gehen Sie auf **Parameter importieren**.
   - Um die Parameter einer einzelnen Funktionalkomponente zu importieren, öffnen Sie in der Konsolenstruktur das Kontextmenü des Knotens dieser Funktionalkomponente und gehen Sie auf **Parameter importieren**.

   Darauf öffnet sich das Begrüßungsfenster des Assistenten für den Parameter-Import.

2. Folgen Sie den Anweisungen in den Fenstern des Assistenten: Geben Sie die Konfigurationsdatei an, aus der Sie die Parameter importieren wollen.

> **Hinweis**
>
> Nachdem Sie allgemeine Parameter für Anti-Virus oder für funktionale Anti-Virus-Komponenten auf dem Server importiert haben, können Sie nicht zu den vorherigen Werten dieser Parameter zurückkehren.

3. Klicken Sie im Fenster **Die Anwendungsparameter sind importiert worden** auf **OK**, um den Assistenten zum Parameter-Import zu schließen.

4. Klicken Sie in der Symbolleiste der Anti-Virus-Konsole auf die Schaltfläche **Aktualisieren**, um die importierten Parameter anzuzeigen.

> **Hinweis**
>
> Anti-Virus importiert keine Kennwörter (Daten von Benutzerkonten für den Start von Aufgaben oder für die Verbindung mit einem Proxyserver) aus einer Datei, die auf einem anderen Computer angelegt wurde oder auf dem gleichen Computer gespeichert wurde, nachdem Anti-Virus auf diesem neu installiert oder aktualisiert wurde. Die Kennwörter müssen nach dem Abschluss des Imports manuell eingegeben werden.

KAPITEL 5. AUFGABEN-VERWALTUNG

In diesem Kapitel stehen die folgenden Informationen:

- Kategorien der Anti-Virus-Aufgaben entsprechend dem Erstellungs- und Ausführungsort (s. Pkt. 5.1 auf S. 52)
- Anlegen einer Aufgabe (s. Pkt. 5.2 auf S. 54)
- Speichern einer Aufgabe nach Ändern der Parameter (s. Pkt. 5.3 auf S. 57)
- Umbenennen einer Aufgabe (s. Pkt. 5.4 auf S. 58)
- Löschen einer Aufgabe (s. Pkt. 5.5 auf S. 58)
- Starten / Anhalten / Fortsetzen / Beenden einer Aufgaben von Hand (s. Pkt. 5.6 auf S. 58)
- Arbeiten mit einem Aufgabenzeitplan (s. Pkt. 5.7 auf S. 59)
- Aufgabenstatistik anzeigen (s. Pkt. 5.8 auf S. 64)
- Zuweisen eines anderen Benutzerkontos für Aufgabenstart (s. Pkt. 5.9 auf S. 65)

5.1. Kategorien der Anti-Virus-Aufgaben

Die Funktionen *Echtzeitschutz*, *Virensuche*, *Update* und *Lizenzschlüsselverwaltung* des Anti-Virus werden durch *Aufgaben* erledigt. Sie können Aufgaben manuell oder nach Zeitplan starten und beenden.

Aufgaben werden nach Erstellungs- und Ausführungsort in *lokale Aufgaben* und *Gruppenaufgaben* unterteilt. Es gibt zwei Kategorien von lokalen Aufgaben: *Systemaufgaben* und *Benutzeraufgaben*.

Aufgaben werden in *lokale Aufgaben* und *Gruppenaufgaben* unterteilt.

Lokale Aufgaben

Lokale Aufgaben werden nur auf dem geschützten Server ausgeführt, für die sie angelegt wurden.

- **Lokale Systemaufgaben** werden automatisch beim Installieren des Anti-Virus angelegt. Sie können die Parameter aller Systemaufgaben ändern, ausgenommen sind die Aufgaben **Untersuchung von Quarantäne-Objekten**, **Untersuchung der Programm-Integrität** und **Rollback der Programm-Datenbanken**. Sie können die Systemaufgaben nicht umbenennen oder löschen. Sie können Systemaufgaben und benutzerdefinierte Aufgaben gleichzeitig starten.

- **Lokale benutzerdefinierte Aufgaben**. In der Anti-Virus-Konsole in der MMC können Sie neue Aufgaben zur Virensuche hinzufügen. In der Administrationskonsole des Programms Kaspersky Administration Kit können Sie neue Aufgaben für die Virensuche, für das Update der Datenbanken, für den Rollback von Datenbank-Updates und für die Update-Verteilung anlegen. Diese Aufgaben nennen sich benutzerdefiniert. Sie können die benutzerdefinierten Aufgaben umbenennen, konfigurieren und löschen. Es können gleichzeitig mehrere benutzerdefinierte Aufgaben gestartet werden.

Gruppenaufgaben

Gruppenaufgaben und globale Aufgaben, die in der Administrationskonsole von Kaspersky Administration Kit angelegt worden sind, werden in der MMC in der Anti-Virus-Konsole dargestellt. Sie werden alle in der Anti-Virus-Konsole als Gruppenaufgaben bezeichnet. Sie können Gruppenaufgaben verwalten und sie aus dem Programm Kaspersky Administration Kit einstellen. In der Anti-Virus-Konsole in der MMC können nur Sie den Status der Gruppenaufgaben anzeigen lassen.

In der Anti-Virus-Konsole werden die Daten zu den Aufgaben angezeigt (s. Beispiel in Abbildung 9).

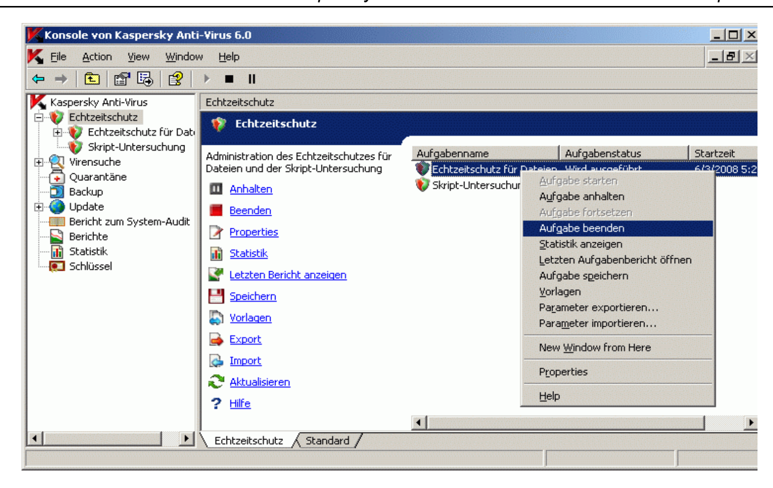


Abbildung 9. Aufgaben des Echtzeitschutzes im Fenster der Anti-Virus-Konsole

Die Befehle für die Aufgabenverwaltung werden im Kontextmenü dargestellt, das sich mit einem Klick der rechten Maustaste auf den Aufgabennamen öffnet.

Die Vorgänge für die Aufgabenverwaltung werden im Bericht zum System-Audit (s. Pkt. 13.3 auf S. 218) festgehalten.

5.2. Anlegen einer Aufgabe

Sie können benutzerdefinierte Aufgaben im Knoten **Virensuche** anlegen. In den anderen Funktionalkomponenten des Anti-Virus ist das Erstellen von benutzerdefinierten Aufgaben nicht vorgesehen.

Um eine neue Aufgabe zur Virensuche zu erstellen, machen Sie Folgendes:

1. In der Konsolenstruktur öffnen Sie das Kontextmenü für den Knoten **Virensuche** und gehen Sie auf **Aufgabe hinzufügen** (s. Abbildung 10).

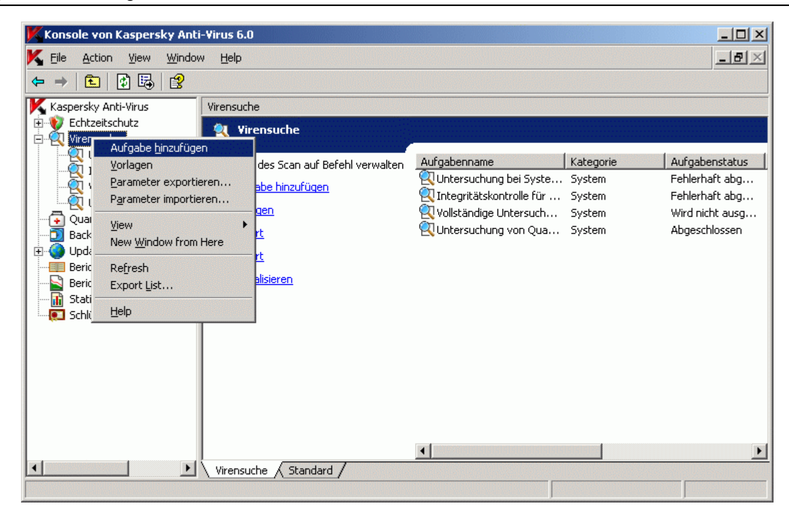


Abbildung 10. Beispiel für Aufgabenerstellung

Es öffnet sich das Dialogfenster **Aufgabe erstellen** (s. Abbildung 11).

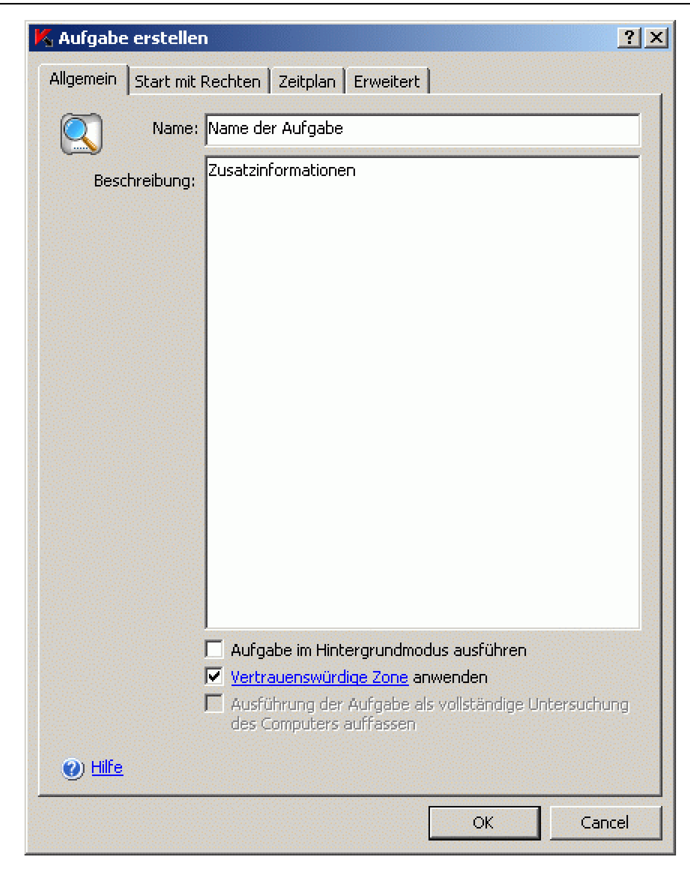


Abbildung 11. Dialogfenster **Aufgabe erstellen**

2. Tragen Sie die folgenden Informationen über die Aufgabe ein:
   - **Name** – Name der Aufgabe, nicht mehr als 100 Zeichen
   - **Beschreibung** – Beliebige Zusatzinformationen zur Aufgabe, nicht mehr als 2000 Zeichen. Im Dialogfenster **Eigenschaften der Aufgabe** werden diese Angaben dann angezeigt.
3. Wenn die Aufgabe im Prozess mit niedriger Priorität ausgeführt werden muss, setzen Sie das Häkchen in **Aufgabe im Hintergrundmodus ausführen** (Details zu den Prioritäten von Anti-Virus-Aufgaben finden Sie in Pkt. 9.3 auf S. 143).

4. Klicken Sie auf die Schaltfläche **OK**. Die Aufgabe wird angelegt. Im Fenster der Konsole erscheint eine Zeile mit den entsprechenden Angaben.

5.3. Speichern einer Aufgabe nach Ändern ihrer Parameter

Sie können die Parameter einer gestarteten und beendeten (angehaltenen) Aufgabe ändern:

- *Wenn Sie die Parameter einer gestarteten Aufgabe geändert haben*: treten in den Aufgaben des Echtzeitschutzes die neue Parameterwerte sofort in Kraft, wenn Sie sie speichern, in den übrigen Aufgaben werden sie beim nächsten Aufgabenstart übernommen.
- *Wenn Sie die Parameter einer beendeten Aufgabe geändert haben*: treten die neuen Parameterwerte in Kraft, wenn Sie sie speichern und die Aufgabe starten.

Um die geänderten Parameter einer Aufgabe zu speichern, öffnen Sie das Kontextmenü mit einem Rechtsklick auf den Aufgabennamen und gehen auf ***Aufgabe speichern****.*

Anmerkung

Wenn Sie nach dem Ändern der Parameter einer Aufgabe in der Konsolenstruktur einen anderen Knoten auswählen und vorher nicht vorsichtshalber auf den Eintrag **Aufgabe speichern** geklickt haben, erscheint das Dialogfenster Speichern der Einstellungen. Sie klicken dort auf die Schaltfläche **Ja**, damit die Parameter der Aufgabe gespeichert werden oder auf **Nein**, damit der Knoten ohne Speichern verlassen wird.

Wie die Parameter einer Aufgabe des **Echtzeitschutzes für Dateien** eingestellt werden, finden Sie in Pkt. 6.2 auf S. 69.

Wie die Parameter einer Aufgabe zur Virensuche eingestellt werden, finden Sie in Pkt. 9.2 auf S. 122.

Das Einstellen der Parameter für Aufgaben zum Update ist in Pkt. 10.5 auf S. 159 näher beschrieben.

5.4. Umbenennen einer Aufgabe

Sie können in der Anti-Virus-Konsole nur benutzerdefinierte Aufgaben umbenennen, Systemaufgaben und Gruppenaufgaben lassen sich nicht umbenennen.

Um eine Aufgabe umzubenennen, machen Sie Folgendes:

1. Öffnen Sie das Kontextmenü des Aufgabennamens und gehen Sie auf **Eigenschaften**.
2. Im Dialogfenster **Eigenschaften** geben Sie den neuen Aufgabenamen im Feld **Name** ein und klicken auf die Schaltfläche **OK**.

Die Aufgabe wird umbenannt. Der Vorgang wird im Bericht zum System-Audit (s. Pkt. 13.3 auf S. 218) festgehalten.

Wie ein Aufgabenzeitplan eingestellt wird, finden Sie in Pkt. 5.7 auf S. 59.

5.5. Löschen einer Aufgabe

Sie können in der Anti-Virus-Konsole nur benutzerdefinierte Aufgaben löschen, Systemaufgaben und Gruppenaufgaben lassen sich nicht löschen.

Um eine Aufgabe zu löschen, machen Sie Folgendes:

1. Öffnen Sie das Kontextmenü des Aufgabennamens und gehen Sie auf **Aufgabe löschen**.
2. Im Dialogfenster **Löschen einer Aufgabe** klicken Sie auf die Schaltfläche **Ja**, um den Vorgang zu bestätigen.

Die Aufgabe wird gelöscht und der Löschvorgang wird im Bericht zum System-Audit (s. Pkt. 13.3 auf S. 218) festgehalten.

5.6. Starten, Anhalten, Fortsetzen, Beenden einer Aufgabe von Hand

Sie können alle Aufgaben anhalten und fortsetzen, ausgenommen sind Aufgaben zum Update.

Um eine Aufgabe zu starten oder anzuhalten oder fortzusetzen oder zu beenden, öffnen Sie das Kontextmenü mit einem Rechtsklick auf den Aufgabenamen

*und gehen Sie auf den gewünschten Eintrag: **Starten**, **Anhalten**, **Fortsetzen** oder **Beenden**.*

Der Vorgang wird ausgeführt. Im Ergebnisfenster ändert sich der Status der Aufgabe. Der Vorgang wird im Bericht zum System-Audit (s. Pkt. 13.3 auf S. 218) festgehalten.

Anmerkung

Wenn Sie eine Aufgabe zur Virensuche anhalten und sie danach fortsetzen, fährt Anti-Virus mit dem Objekt fort, bei dem die Aufgabe zuletzt angehalten wurde.

5.7. Arbeit mit Aufgabenzeitplan

In diesem Abschnitt stehen die folgenden Informationen:

- Einstellen eines Aufgabenzeitplans (s. Pkt. 5.7.1 auf S. 59)
- Aktivieren / Deaktivieren eines eingestellten Aufgabenzeitplans (s. Pkt. 5.7.2 auf S. 64)

Die Parameter eines Zeitplans werden in Pkt. B.2 auf S. 389 näher erläutert.

5.7.1. Aufgabenzeitplan einstellen

In der Anti-Virus-Konsole können Sie einen Zeitplan für lokale Systemaufgaben und benutzerdefinierte Aufgaben einstellen. Für Gruppenaufgaben können Sie keinen Zeitplan eingeben.

Die Zeitplan-Parameter werden in Pkt. B.2 auf S. 389 näher beschrieben.

Um die Parameter eines Aufgabezeitplans einzustellen, machen Sie Folgendes:

1. Öffnen Sie das Kontextmenü für den Namen der Aufgabe, deren Zeitplan Sie anpassen möchten, und wählen Sie den Befehl **Eigenschaften**.
2. Im Dialogfenster **Eigenschaften: <Aufgabe>** (s. Abbildung 12) aktivieren Sie auf der Registerkarte **Zeitplan** den Start der Aufgabe nach Zeitplan: Setzen Sie das Häkchen im Kontrollkästchen **Aufgabe nach Zeitplan starten**.

Hinweis

Die Felder mit den Zeitplanparametern der Systemaufgabe stehen nicht zur Verfügung, wenn der Start dieser Systemaufgabe durch eine Richtlinie des Programms Kaspersky Administration Kit deaktiviert wurde (s. Pkt. 19.4 auf S. 297).

3. Konfigurieren Sie die Parameter des Zeitplans je nach Ihren Wünschen.

   a) Geben Sie die Starthäufigkeit an, mit der die Aufgabe gestartet wird (s. Pkt. B.2.1 auf S. 390): Wählen Sie aus der Liste **Startfrequenz** einen der folgenden Werte aus: **Stündlich**, **Täglich**, **Wöchentlich**, **Bei Programmstart**, **Nach dem Datenbank-Update**:

      - Wenn Sie **Stündlich** gewählt haben, geben Sie den Wert **Jede <Zahl> Stunde** in der Parametergruppe **Parameter für Aufgabenstart** an.

      - Wenn Sie **Täglich** gewählt haben, geben Sie die Anzahl der Tage im Feld **Alle <Zahl> Tage** in der Parametergruppe **Parameter für Aufgabenstart** an.

      - Wenn Sie **Wöchentlich** gewählt haben, geben Sie die Anzahl der Wochen im Feld **Jede <Zahl> Woche** in der Parametergruppe **Parameter für Aufgabenstart** an. Legen Sie fest, an welchen Wochentagen die Aufgabe gestartet wird (standardmäßig wird eine Aufgabe montags gestartet).

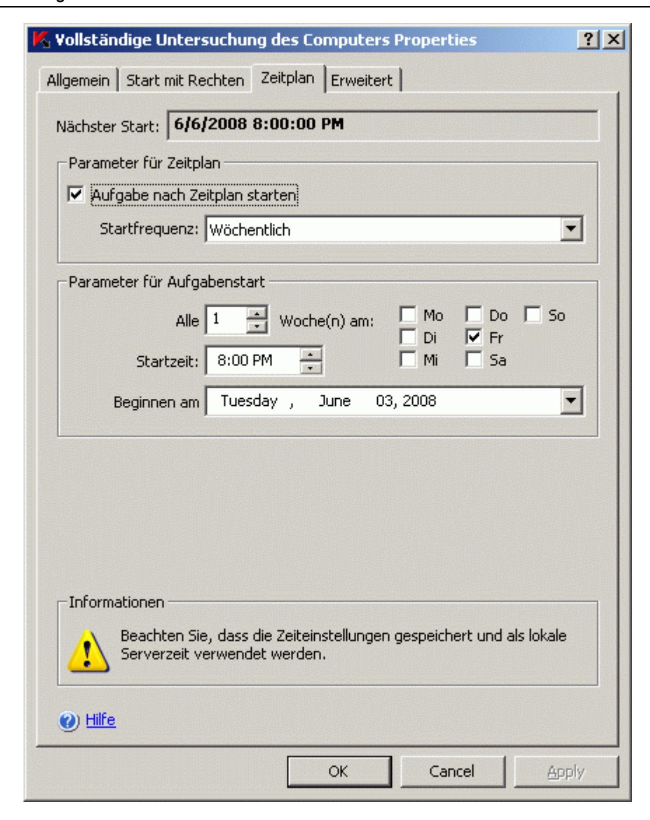


Abbildung 12. Beispiel für das Dialogfenster **Eigenschaften: <Aufgabe>** mit dem Wert **Startfrequenz: Wöchentlich**.

b) Im Feld **Startzeit** geben Sie Datum und Uhrzeit des Aufgabenstarts ein.

c) Im Feld **Beginnen am** tragen Sie das Startdatum des Zeitplans ein (s. Pkt. B.2.2 auf S. 391).

Anmerkung

Nachdem Sie das die Startfrequenz der Aufgabe, die Uhrzeit für den ersten Aufgabenstart und das Datum, ab dem der Zeitplan gelten soll, angegeben haben, wird im oberen Bereich des Dialogfensters im Feld **Nächster Start** der *berechnete Zeitpunkt des nächsten Aufgabenstarts* angezeigt. Aktualisierte Informationen über den nächsten Startzeitpunkt werden jedes Mal angezeigt, wenn das Dialogfenster **Eigenschaften: <Aufgabe>** auf der Registerkarte **Zeitplan** geöffnet wird.

Der Wert **Start der Aufgabe ist aufgrund der Systemrichtlinie verboten** wird im Feld **Nächster Start** angezeigt, wenn der Start von zeitgesteuerten Systemaufgaben durch die Parameter der geltenden Richtlinie des Programms Kaspersky Administration Kit untersagt wird (Detail s. Pkt. 19.4 auf S. 297).

4. Auf der Registerkarte **Erweitert** (s. Abbildung 13) stellen Sie die übrigen Zeitplan-Parameter je nach Ihren Wünschen ein.

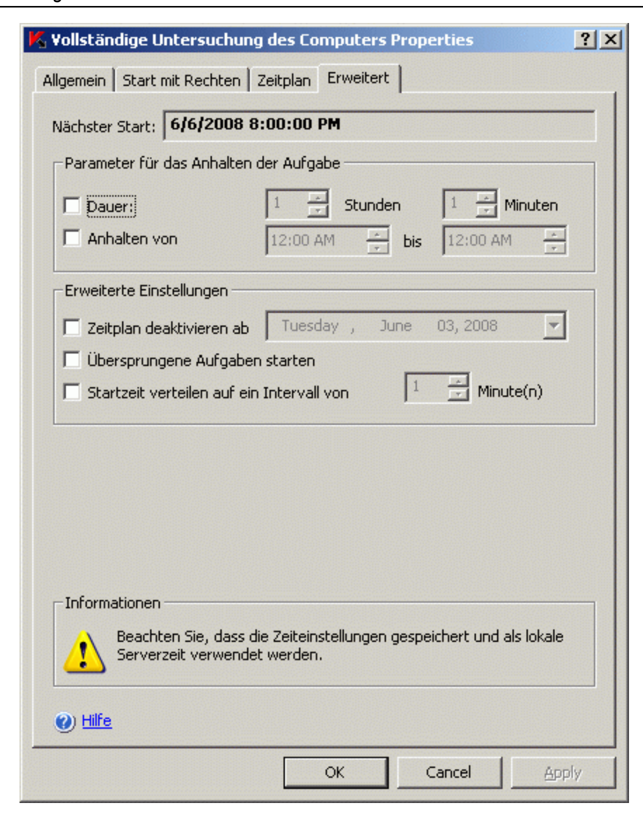


Abbildung 13. Dialogfenster **Eigenschaften: <Aufgabe>**, Registerkarte **Erweitert**

a) Um eine maximale Dauer der Aufgabenausführung anzugeben, tragen Sie in der Gruppe **Parameter für das Anhalten der Aufgabe**, im Feld **Dauer** die gewünschte Anzahl der Stunden und Minuten (s. Pkt. B.2.4 auf S. 393).

b) Um einen Zeitabschnitt innerhalb von Tagen einzutragen, in dem die Aufgabenausführung angehalten wird, geben Sie in der Gruppe **Parameter für das Anhalten der Aufgabe** im Feld **Anhalten von … bis** die Anfangs- und Endwerte an (s. Pkt. B.2.5 auf S. 393).

c) Um ein Datum anzugeben, ab dem der Zeitplan außer Kraft tritt, setzen Sie das Häkchen in **Zeitplan deaktivieren ab** und wählen Sie mit dem Dialogfenster **Kalender** das Datum, von dem an der Zeitplan nicht mehr gültig ist (s. Pkt. B.2.5 auf S. 393).

d) Um den Start von übersprungenen Aufgaben zu aktivieren, setzen Sie das Häkchen in **Übersprungene Aufgaben starten** (s. Pkt. B.2.6 auf S. 394).

e) Um den Gebrauch des Parameters **Startzeit verteilen** zu aktivieren, setzen Sie das Häkchen in **Startzeit verteilen auf ein Intervall von** und geben Sie den Parameterwert in Minuten ein (s. Pkt. B.2.7 auf S. 395).

5. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen im Dialogfenster **Eigenschaften: <Aufgabe>** zu speichern.

5.7.2. Aufgabe nach Zeitplan aktivieren und deaktivieren

Nachdem Sie einen Aufgabenzeitplan eingestellt haben, können Sie ihn aktivieren oder deaktivieren. Wenn Sie einen Zeitplan deaktivieren, werden seine Werte (Startintervall, Startzeit und weitere) nicht gelöscht, und Sie können den Zeitplan bei Bedarf erneut aktivieren.

Um einen Zeitplan zu aktivieren oder zu deaktivieren, machen Sie Folgendes:

1. Öffnen Sie das Kontextmenü mit einem Rechtsklick auf den Namen der Aufgabe, deren Zeitplan Sie aktivieren oder deaktivieren wollen, und gehen Sie auf **Eigenschaften**.

2. Im Dialogfenster **Eigenschaften: <Aufgabe>** führen Sie in der Parameter-Gruppe **Parameter für Zeitplan** eine der folgenden Aktionen aus:

   - Um den Zeitplan zu aktivieren, setzen Sie das Häkchen in **Aufgabe nach Zeitplan starten**.

   - Um den Zeitplan zu deaktivieren, entfernen Sie das Häkchen im Kontrollkästchen **Aufgabe nach Zeitplan starten**.

3. Klicken Sie auf die Schaltfläche **OK**.

5.8. Anzeigen einer Aufgabenstatistik

Solange eine Aufgabe ausgeführt wird, können Sie die Detailinformationen zur Ausführung einer Aufgabe seit dem Aufgabenstart bis jetzt in Echtzeit anzeigen lassen, im Dialogfenster **Statistik**.

Die Information im Dialogfenster **Statistik** wird sichtbar, wenn Sie die Aufgabe anhalten. Nach dem die Aufgabe beendet oder angehalten wird können Sie diese Information im detaillierten Protokoll über Ereignisse in der Aufgabe (s. Pkt. 13.2.4 auf S. 210).

*Um die Statistik einer Aufgabe anzuzeigen, öffnen Sie im Konsolenfenster das Kontextmenü mit einem Rechtsklick auf den Namen der Aufgabe, deren Statistik Sie anzeigen lassen wollen, und gehen Sie auf **Statistik**.*

5.9. Benutzerkonten für Aufgabenstart

In diesem Abschnitt stehen die folgenden Informationen:

- Verwenden eines anderen Benutzerkontos für Aufgabenstart (s. Pkt. 5.9.1 auf S. 65)
- Zuweisen eines Benutzerkontos für Aufgabenstart (s. Pkt. 5.9.2 auf S. 66)

5.9.1. Zuweisen eines Benutzerkontos für Aufgabenstart

Sie können ein Benutzerkonto angeben, mit deren Berechtigungen eine ausgewählte Aufgabe in einer beliebigen Funktionalkomponente des Anti-Virus, bis auf die Komponente **Echtzeitschutz**, gestartet wird.

Als Standard werden alle Aufgaben, außer den Aufgaben des Echtzeitschutzes, unter dem Benutzerkonto **Lokales System** (**SYSTEM**) ausgeführt. Bei den Aufgaben des Echtzeitschutzes fängt Anti-Virus das zu untersuchende Objekt ab, wenn eine Anwendung darauf zugreift, und verwendet für den Zugriff auf das Objekt die Rechte dieser Anwendung.

Sie müssen in den folgenden Fällen ein anderes Benutzerkonto mit ausreichenden Zugriffsrechten zuweisen:

- in der Aufgabe zum Update, wenn Sie als Updatequelle einen gemeinsamen Ordner auf einem anderen Netzwerkcomputer angegeben haben.
- in der Aufgabe zum Update, wenn für Zugriff auf die Updatequelle ein Proxyserver mit der integrierten Authentizitätsprüfung von Microsoft Windows zwischengeschaltet ist (NTLM-authentication).

- in den Aufgaben zur Virensuche, wenn das Benutzerkonto **Lokales System** (**SYSTEM**) nicht die Zugriffsrechte auf die zu untersuchenden Objekte hat (zum Beispiel für die Dateien in gemeinsamen Ordnern im Netzwerk).

Hinweis

Sie können unter dem Benutzerkonto **Lokales System** (**SYSTEM**) Aufgaben zum Update und zur Virensuche starten, in denen Anti-Virus auf gemeinsame Ordner eines anderen Netzwerkcomputers zugreift, wenn dieser Computer in der gleichen Domäne angemeldet ist wie der geschützte Server. In diesem Fall muss das Benutzerkonto **Lokales System** (**SYSTEM**) Zugriffsrechte auf diese Ordner besitzen. Anti-Virus wird mit den Rechten des Benutzerkontos **Domänenname\Computername$** auf den Computer zugreifen.

5.9.2. Angabe eines Benutzerkontos für Aufgabenstart

Um ein anderes Benutzerkonto für den Aufgabenstart zuzuweisen, machen Sie Folgendes:

1. Öffnen Sie das Kontextmenü mit einem Rechtsklick auf den Namen der Aufgabe und gehen Sie auf **Eigenschaften**.
2. Öffnen Sie im Dialogfenster **Eigenschaften: <Aufgabe>** die Registerkarte **Start mit Rechten** (s. Abbildung 14).

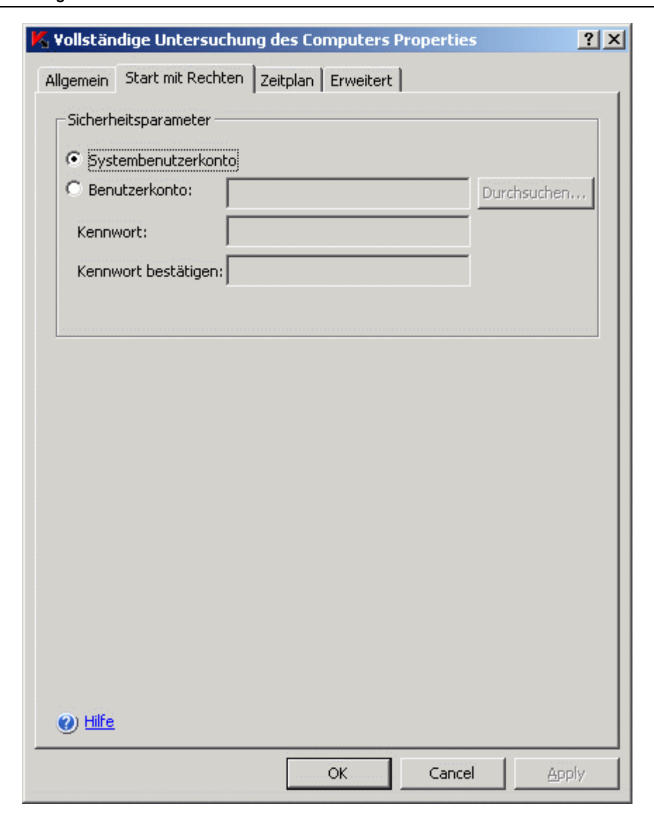


Abbildung 14. Dialogfenster **Start mit Rechten**

3. Nehmen Sie im Dialogfenster **Start mit Rechten** folgende Einstellungen vor:

   a) Wählen Sie das **Benutzerkonto** aus.

   b) Tragen Sie den Namen und das Kennwort des Benutzers ein, dessen Konto Sie verwenden wollen.

   > **Anmerkung**
   >
   > Der von Ihnen ausgewählte Benutzer muss auf dem geschützten Server oder in einer dort gelegenen Domäne angemeldet sein.

   c) Klicken Sie auf die Schaltfläche **OK**.

KAPITEL 6. ECHTZEITSCHUTZ

In diesem Kapitel stehen die folgenden Informationen:

- Aufgaben des Echtzeitschutzes (s. Pkt. 6.1 auf S. 68)
- Einstellen von Aufgaben des **Echtzeitschutzes für Dateien** (s. Pkt. 6.2 auf S. 69)
- Statistik einer Aufgabe des **Echtzeitschutzes für Dateien** (s. Pkt. 6.3 auf S. 91)
- Einstellen der Aufgabe **Skript-Untersuchung**: Aktionen für verdächtige Skripte auswählen (s. Pkt. 6.4 auf S. 93)
- Statistik einer Aufgabe der **Skript-Untersuchung** (s. Pkt. 6.5 auf S. 95)

6.1. Aufgaben des Echtzeitschutzes

Im Anti-Virus sind zwei Systemaufgaben des Echtzeitschutzes vorgesehen: **Echtzeitschutz für Dateien** und **Skript-Untersuchung**. Details zur Funktion *Echtzeitschutz für Dateien* finden Sie in Pkt. 1.1.1 auf S. 14.

Standardmäßig werden die Aufgaben des Echtzeitschutzes automatisch beim Start des Anti-Virus aufgerufen. Sie können diese Aufgaben beenden und wieder starten und / oder ihren Zeitplan einstellen. Außerdem können Sie die Aufgabe des Echtzeitschutzes anhalten und fortsetzen, wenn die Objekt-Untersuchung bei Zugriff kurz unterbrochen werden muss, beispielsweise bei einer Daten-Replikation.

Sie können eine Aufgabe des **Echtzeitschutzes für Dateien** in folgender Hinsicht anpassen: den Schutzbereich und die Sicherheitsparameter für ausgewählte Knoten festlegen, das Sperren des Zugriffs von Computern veranlassen, die vertrauenswürdige Zone übernehmen (s. Pkt. 6.2 auf S. 69).

Wenn eine Aufgabe der **Skript-Untersuchung** ausgeführt wird, werden die Skripte unterdrückt, die Anti-Virus als gefährlich erkennt. Wenn Anti-Virus ein Skript als verdächtig einstuft, dann führt er die von Ihnen ausgewählte Aktion aus: Er gestattet die Ausführung oder er unterbindet sie. Wie die Ausführung von verdächtigen Skripten unterbunden oder gestattet werden kann, finden Sie in Pkt. 6.4 auf S. 93.

6.2. Einstellen der Aufgabe *Echtzeitschutz für Dateien*

Standardmäßig hat die Systemaufgabe **Echtzeitschutz für Dateien** Parameter, die in der Tabelle 2 aufgezählt sind. Sie können die Werte dieser Parameter ändern und die Aufgabe damit einstellen.

Tabelle 2. Parameter der Aufgabe **Echtzeitschutz für Dateien** in der Grundeinstellung

Parameter	Standardwert	Beschreibung
Sicherheitsbereich	gesamter Server	Sie können den Schutzbereich einschränken (Pkt. 6.2.1 auf S. 72).
Parameter für Sicherheit	Einheitlich für den gesamten Schutzbereich, entspricht der Sicherheitsstufe **Empfohlen**	Sie können für ausgewählte Knoten im Baum der File-Server-Ressourcen: • eine andere vordefinierte Sicherheitsstufe auswählen (s. Pkt. 6.2.2.1 auf S. 79) • manuell die Parameter für Sicherheit ändern (s. Pkt. 6.2.2.2 auf S. 82). Sie können die Parameter für Sicherheit des ausgewählten Knotens in eine Vorlage speichern, um sie später für andere Knoten zu übernehmen (s. Pkt. 6.2.2.3 auf S. 86).
Schutzmodus für Objekte	Beim Öffnen und Ändern	Sie können den Schutzmodus für Objekte bestimmen, d. h., bei welchen Zugriffsarten auf Objekte Anti-Virus diese überprüfen wird. Wie ein Schutzmodus eingestellt wird, finden Sie in Pkt. 6.2.3 auf S. 90. Details zu den Schutzmodi für Objekte finden Sie in Pkt. B.3.1 auf S. 396.

Parameter	Standardwert	Beschreibung
Zugriff von Computern sperren	Ausgeschaltet	Sie können den Zugriff von Computern auf den geschützten Server sperren, wenn er mit infizierten oder verdächtigen Objekten auf dem geschützten Server zu schreiben versucht (s. Kapitel 7 auf S. 96).
Vertrauenswürdige Zone	Wird verwendet. Ausgeschlossen werden Programme zur Remote-Administration **RemoteAdmin** und Dateien, die von der Firma Microsoft empfohlen werden, falls Sie bei der Installation von Anti-Virus die Optionen **Bedrohungen nach Maske not-a-virus:RemoteAdmin* zu Ausnahmen hinzufügen** und **Dateien zu Ausnahmen hinzufügen, die Microsoft empfiehlt** gewählt haben.	Einheitliche Liste der Ausnahmen, die Sie in ausgewählten Aufgaben zur Virensuche und in der Aufgabe **Echtzeitschutz für Dateien** verwenden können. Kapitel 8 auf S. 109 enthält Informationen über das Erstellen und die Verwendung der vertrauenswürdigen Zone.

*Um die Aufgabe **Echtzeitschutz für Dateien** einzustellen, machen Sie Folgendes:*

1. In der Konsolenstruktur klappen Sie den Knoten **Echtzeitschutz** auf.
2. Wählen Sie den eingebetteten Knoten **Echtzeitschutz für Dateien** aus.

   Im Ergebnisfenster wird der Baum der File-Server-Ressourcen sowie das Dialogfenster **Sicherheitsstufe** (Standardmodus) (s. Abbildung 15) dargestellt.

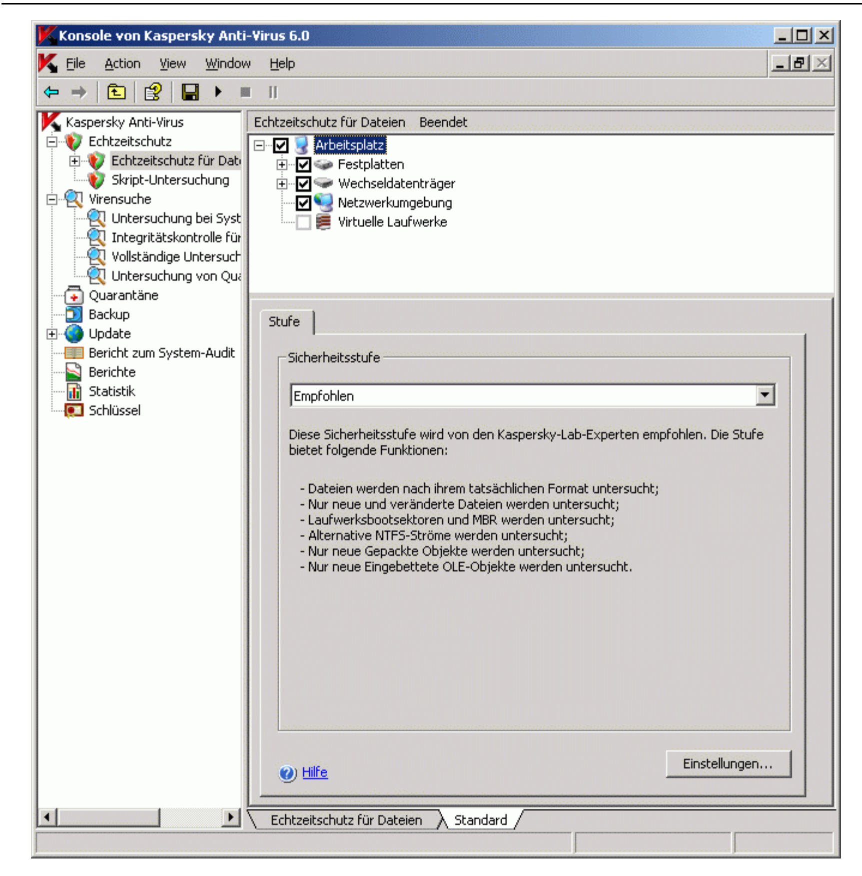


Abbildung 15. Geöffneter Aufgabe **Echtzeitschutz für Dateien**

3. Bei Bedarf stellen Sie die Parameter für die Aufgabe ein.
4. Öffnen Sie das Kontextmenü mit einem Rechtsklick auf den Namen der Aufgabe und gehen Sie auf **Aufgabe speichern**, um die Änderungen in der Aufgabe zu speichern.

Näheres dazu, wie,

- eine Aufgabe von Hand starten / anhalten / fortsetzen / beenden, s. Pkt. 5.6 auf S. 58
- eine Aufgabe nach Zeitplan gestartet werden kann, finden Sie in Pkt. 5.7 auf S. 59.

6.2.1. Schutzbereich in der Aufgabe *Echtzeitschutz für Dateien*

In diesem Abschnitt stehen die folgenden Informationen:

- Erstellen eines Schutzbereiches in der Aufgabe *Echtzeitschutz für Dateien* (s. Pkt. 6.2.1.1 auf S. 72)
- wie Sie welche Serverbereiche in den Schutzbereich aufnehmen können (s. Pkt. 6.2.1.2 auf S. 73)
- Schutzbereich anlegen: Einzelne Serverbereiche ausschließen oder aufnehmen (s. Pkt. 6.2.1.3 auf S. 74)
- virtuelle Schutzbereiche – Datenträger, Ordner und Dateien, die temporär auf dem Server beobachtet werden, sowie Ordner und Dateien, die dynamisch auf dem Server von verschiedenen Anwendungen und Diensten bei ihrer Ausführung angelegt werden (s. Pkt. 6.2.1.4 auf S. 76)
- wie ein virtueller Schutzbereich angelegt wird (s. Pkt. 6.2.1.5 auf S. 76).

6.2.1.1. Schutzbereich in der Aufgabe *Echtzeitschutz für Dateien* erstellen

Wenn die Aufgabe **Echtzeitschutz für Dateien** mit Parametern ausgeführt wird, die ein Standardwert sind, untersucht Anti-Virus alle Objekte des Server-Dateisystems. Wenn aus Sicherheitsgründen nicht alle Objekte untersucht werden müssen, können Sie den Schutzbereich einschränken.

In der Anti-Virus-Konsole ist der Schutzbereich ein Baum der File-Server-Ressourcen, die Anti-Virus untersuchen kann.

Die Knoten im Baum der File-Server-Ressourcen werden auf folgende Weise dargestellt:

Der Knoten ist im Schutzbereich.

Der Knoten ist nicht im Schutzbereich.

Mindestens ein in diesem Knoten eingebetteter Knoten ist nicht im Schutzbereich oder die Sicherheitsparameter des eingebetteten Knotens (der Knoten) unterscheiden sich von den Sicherheitsparametern dieses Knotens.

Beachten Sie, dass der Mutterknoten mit dem Symbol gekennzeichnet wird, wenn Sie alle eingebetteten Knoten auswählen, jedoch der Mutterknoten selbst wird nicht so markiert. In diesem Fall werden Dateien und Ordner,

die in diesem Knoten eingebettet sind, nicht automatisch in den Schutzbereich übernommen. Um sie zu übernehmen, können Sie deren Mutterknoten in den Schutzbereich aufnehmen. Oder Sie können sie "virtuell" in der Anti-Virus-Konsole anlegen und sie manuell dem Schutzbereich hinzufügen.

Die Namen der virtuellen Knoten in einem Schutzbereich werden mit Schrift in blauer Farbe angezeigt.

6.2.1.2. Vordefinierte Schutzbereiche

Wenn Sie die Aufgabe **Echtzeitschutz für Dateien** öffnen, wird im Ergebnisfenster der Baum der File-Server-Ressourcen dargestellt (s. Abbildung 16).

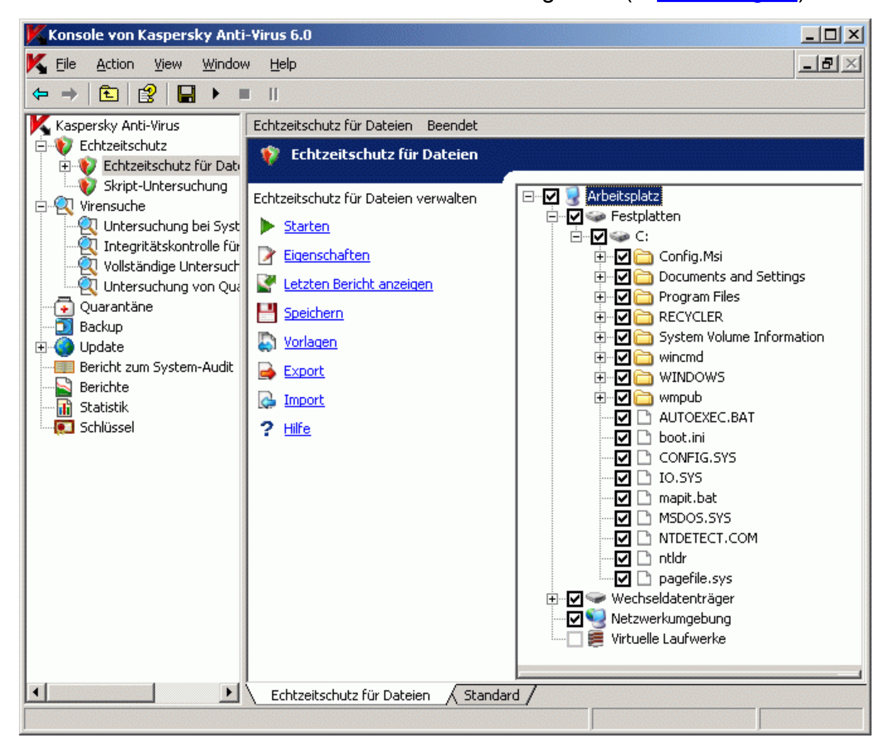


Abbildung 16. Beispiel für Baum der File-Server-Ressourcen in der Anti-Virus-Konsole

Anmerkung

Der Baum der File-Server-Ressourcen zeigt die Knoten an, für welche Sie die Lese-Rechte besitzen je nach den Sicherheitseinstellungen in Microsoft Windows haben.

Der Baum der File-Server-Ressourcen enthält die folgenden vordefinierten Schutzbereiche:

- **Festplatten** Anti-Virus untersucht Dateien auf den Festplatten-Datenträgern des Servers.
- **Wechseldatenträger**. Anti-Virus untersucht Dateien auf den Wechseldatenträgern, zum Beispiel auf CD-ROMs oder USB-Sticks.
- **Netzwerkumgebung**. Anti-Virus untersucht Dateien, die in den Netzwerkordnern erfasst sind bzw. die von Anwendungen abgefragt werden, die auf dem Server laufen. Er untersucht keine Dateien in Netzwerkordnern, wenn sich Programme von anderen Rechnern Zugriff verschaffen wollen.
- **Virtuelle Laufwerke**. Sie können in den Schutzbereich dynamische Ordner und Dateien sowie Datenträger aufnehmen, die temporär vom Server überwacht werden, beispielsweise allgemeine Datenträger eines Clusters (Anlegen eines *virtuellen Schutzbereiches*).

Anmerkung

Pseudo-Datenträger, die mit SUBST erzeugt worden sind, werden im Baum der File-Server-Ressourcen in der Anti-Virus-Konsole nicht dargestellt. Um Objekte auf einem Pseudo-Datenträger in den Schutzbereich zu übernehmen, beziehen Sie in den Schutzbereich den Ordner auf dem Server ein, mit dem der Pseudo-Datenträger verknüpft ist.

Die angeschlossenen Netzwerk-Datenträger werden im Baum der File-Server-Ressourcen nicht dargestellt. Um Objekte auf dem Netzwerk-Datenträger in den Schutzbereich zu übernehmen, geben Sie den Pfad zum Ordner, der diesem Netzwerk-Datenträger entspricht, im UNC-Format (Universal Naming Convention) ein.

6.2.1.3. Schutzbereich erstellen

Um einen Schutzbereich anzulegen, machen Sie Folgendes:

1. Öffnen Sie die Aufgabe **Echtzeitschutz für Dateien**.
2. Führen Sie im Ergebnisfenster im Baum der File-Server-Ressourcen die folgenden Aktionen aus:

- Zum Ausschließen eines einzelnen Knotens aus dem Schutzbereich klappen Sie den Baum der Dateiressourcen auf, um den gewünschten Knoten darzustellen, und Sie entfernen das Häkchen neben seinen Namen.
- Um nur diejenigen Knoten auszuwählen, die Sie zum Schutzbereich hinzufügen wollen, entfernen Sie das Häkchen vor **Arbeitsplatz**, und dann:
    - wenn Sie alle Datenträger eines Typs in den Schutzbereich nehmen wollen, setzen Sie das Häkchen neben dem Namen des gewünschten Datenträgertyps (z. B., um alle Wechseldatenträger auf dem Server einzuschließen, setzen Sie Häkchen **Wechseldatenträger**)
    - wenn Sie einen einzelnen Datenträger eines gewünschten Typs in den Schutzbereich nehmen wollen, klappen Sie den Knoten auf, der die Liste mit den Datenträgern der gewünschten Typs enthält, und setzen Sie das Häkchen neben dem Namen des Datenträgers. Um zum Beispiel den Wechseldatenträger **F:** auszuwählen, klappen Sie den Knoten **Alle Wechseldatenträger** auf und setzen Sie das Häkchen für den Datenträger **F:**.
    - wenn Sie nur einen einzelnen Ordner auf einem Datenträger in den Schutzbereich nehmen wollen, klappen Sie den Baum der File-Server-Ressourcen auf, um den Ordner anzuzeigen, den Sie in den Schutzbereich übernehmen wollen, und setzen Sie das Häkchen neben dessen Namen. Auf die gleiche Weise können Sie auch Dateien in den Schutzbereich aufnehmen.

3. Öffnen Sie das Kontextmenü mit einem Rechtsklick auf den Namen der Aufgabe und gehen Sie auf **Aufgabe speichern**, um die Änderungen an der Aufgabe zu speichern.

Anmerkung

Sie können die Aufgabe **Echtzeitschutz für Dateien** erst starten, wenn mindestens ein Knoten im Baum der File-Server-Ressourcen in den Schutzbereich übernommen worden ist.

Anmerkung

Wenn Sie einen ungültigen Schutzbereich angeben, Sie setzen beispielsweise verschiedene Sicherheitsparameterwerte für viele einzelne Knoten im Baum der File-Server-Ressourcen, so kann dadurch die Untersuchung der Objekte bei Zugriff etwas verlangsamt werden.

6.2.1.4. Virtuelle Schutzbereiche

Anti-Virus kann nicht nur vorhandene Ordner und Dateien auf Festplatten und Wechseldatenträgern untersuchen, sondern auch Datenträger, die vom Server temporär überwacht werden, beispielsweise allgemeine Datenträger eines Clusters sowie Ordner und Dateien, die von verschiedenen Anwendungen und Diensten dynamisch auf dem Server angelegt werden.

Wenn Sie alle Objekte des Servers in den Schutzbereich übernommen haben, dann gehören auch diese dynamischen Knoten automatisch zum Schutzbereich. Sollten Sie jedoch spezielle Parameterwerte für die Sicherheit dieser dynamischen Knoten eingeben wollen oder Sie haben nicht den gesamten Server unter Echtzeitschutz gestellt, sonder nur einzelne Bereiche, dann muss, um dynamische Datenträger, Ordner und Dateien in den Schutzbereich übernehmen zu können, vorsichtshalber in der Anti-Virus-Konsole ein *virtueller Schutzbereich* eingerichtet werden. Die von Ihnen erzeugten Datenträger, Ordner und Dateien stehen nur in der Anti-Virus-Konsole, nicht aber in der Struktur des Dateisystems für den geschützten Server.

Wenn Sie einen Schutzbereich erstellen und alle eingebetteten Ordner oder Dateien markieren, nicht aber das übergeordnete Verzeichnis, dann werden die dynamischen Ordner oder Dateien, die sich darin befinden, nicht automatisch in den Schutzbereich übernommen. Sie müssen ihn "virtuell" in der Anti-Virus-Konsole anlegen und ihn manuell dem Schutzbereich hinzufügen.

Das Erstellen eines virtuellen Schutzbereiches in der Aufgabe **Echtzeitschutz für Dateien** finden Sie in Pkt. 6.2.1.5 auf S. 76.

Das Erstellen eines virtuellen Schutzbereiches in der Aufgabe **Virensuche** finden Sie in Pkt. 9.2.1.5 auf S. 129.

6.2.1.5. Virtuelle Schutzbereiche erstellen: Dynamische Datenträger, Ordner und Dateien in Schutzbereich übernehmen

Um einen virtuellen Datenträger zum Schutzbereich hinzuzufügen, machen Sie Folgendes:

1. In der Konsolenstruktur klappen Sie den Knoten **Echtzeitschutz** auf und gehen auf den eingebetteten Knoten **Echtzeitschutz für Dateien**.

2. Im Ergebnisfenster öffnen Sie im Baum der File-Server-Ressourcen das Kontextmenü für den Knoten **Virtuelle Laufwerke** und in der Liste mit den verfügbaren Namen wählen Sie einen Namen für den anzulegenden virtuellen Datenträger (s. Abbildung 17).

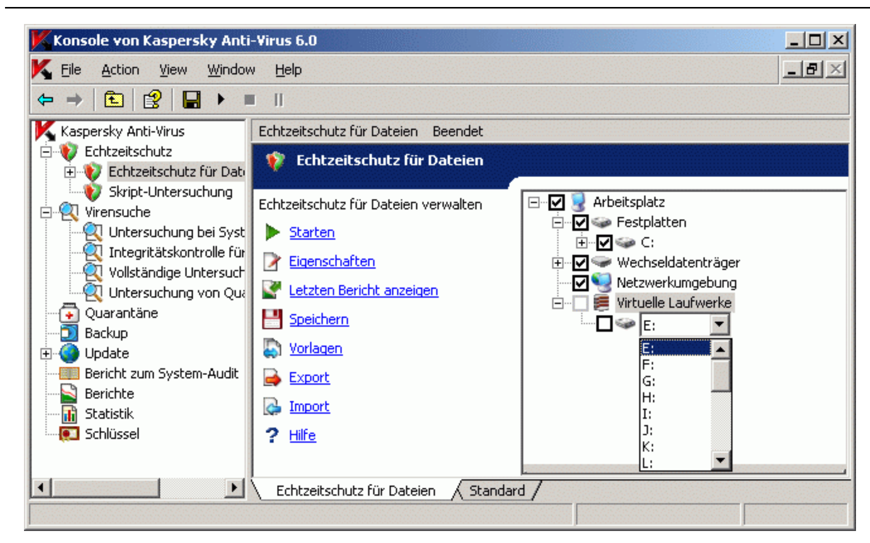


Abbildung 17. Namen für anzulegenden virtuellen Datenträger auswählen

3. Setzen Sie das Häkchen neben dem hinzugefügten Datenträger, um diesen Datenträger in den Schutzbereich zu übernehmen.

4. Öffnen Sie das Kontextmenü mit einem Rechtsklick auf den Namen der Aufgabe und gehen Sie auf **Aufgabe speichern**, um die Änderungen in der Aufgabe zu speichern.

Um einen virtuellen Ordner oder eine virtuelle Datei zum Schutzbereich hinzuzufügen, machen Sie Folgendes:

1. In der Konsolenstruktur klappen Sie den Knoten **Echtzeitschutz** auf und gehen auf den eingebetteten Knoten **Echtzeitschutz für Dateien**.

2. Im Ergebnisfenster öffnen Sie im Baum der File-Server-Ressourcen mit der rechten Maustaste das Kontextmenü des Knotens, in den Sie einen Ordner oder eine Datei einfügen wollen, und gehen auf **Virtuellen Ordner hinzufügen** oder **Virtuelle Datei hinzufügen**.

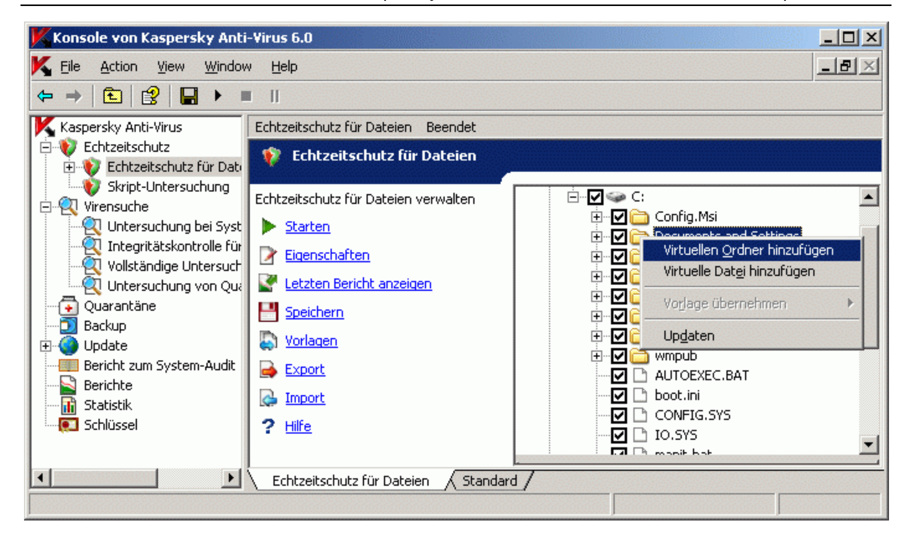


Abbildung 18. Virtuellen Ordner hinzufügen

3. In das Eingabefeld tragen Sie den Namen für den Ordner (die Datei) ein. Bei der Angabe des Dateinamens können Sie seine Maske mit Hilfe der Sonderzeichen * und ? eingeben.

4. In der Zeile mit dem Namen der erstellten Ordners (Datei) setzen Sie das Häkchen, um den Ordner (die Datei) in den Schutzbereich zu übernehmen.

5. Öffnen Sie das Kontextmenü mit einem Rechtsklick auf den Namen der Aufgabe und gehen Sie auf **Aufgabe speichern**, um die Änderungen in der Aufgabe zu speichern.

6.2.2. Parameter für Sicherheit einstellen

Sie können die Parameter für Sicherheit bei einem ausgewählten Knoten im Baum der File-Server-Ressourcen auf die folgende Weise einstellen:

- Auswählen unter einer der drei vordefinierten Sicherheitsstufen (Maximales Tempo, Empfohlen oder Maximale Sicherheit) (s. Pkt. 6.2.2.1 auf S. 79)
- manuelles Ändern der Parameter für Sicherheit (s. Pkt. 6.2.2.2 auf S. 82).

Sie können die Parameter für Sicherheit des ausgewählten Knotens in eine Vorlage speichern, um später diese Vorlage für andere Knoten zu übernehmen (s. Pkt. 6.2.2.3 auf S. 86).

6.2.2.1. Vordefinierte Sicherheitsstufen in der Aufgabe *Echtzeitschutz für Dateien* auswählen

Für ausgewählte Knoten im Baum der File-Server-Ressourcen können Sie eine der vordefinierten Sicherheitsstufen übernehmen: a) maximales Tempo, b) empfohlen und c) maximale Sicherheit. Jede Stufe hat eigene Parameterwerte für die Sicherheit. Die Parameterwerte für die vordefinierten Sicherheitsstufen stehen in der Tabelle 3 auf S. 79.

Maximales Tempo

Sie können die Sicherheitsstufe **Maximales Tempo** auf dem Server aktivieren, wenn in Ihrem Netzwerk neben dem Anti-Virus auf den Servern und Workstations zusätzliche Maßnahmen für die Computersicherheit getroffen worden sind, beispielsweise Firewalls installiert wurden und Sicherheitsrichtlinien für die Netzwerkbenutzer in Kraft sind.

Empfohlen

Die Sicherheitsstufe **Empfohlen** gilt in der Grundeinstellung. Diese Stufe ist nach Empfehlungen der Kaspersky-Lab-Experten für den Schutz von Dateiservern in den meisten Netzwerken ausreichend. Sie sorgt für eine optimale Qualität und die Produktivität der geschützten Server kann gut beeinflusst werden.

Maximale Sicherheit

Entscheiden Sie sich für die Sicherheitsstufe **Maximale Sicherheit**, wenn Sie sehr hohe Vorgaben für die Computersicherheit in einem Netzwerk haben.

Tabelle 3. Vordefinierte Sicherheitsstufen und entsprechende Parameterwerte für Sicherheit

Parameter	**Sicherheitsstufe**		
	Maximales Tempo	**Empfohlen**	**Maximale Sicherheit**
Zu untersuchende Objekte (s. B.3.2 auf S. 397)	nach Erweiterung	Nach Format	Nach Format

Parameter	**Sicherheitsstufe**		
	Maximales Tempo	**Empfohlen**	**Maximale Sicherheit**
Nur neue und veränderte Objekte untersuchen (s. Pkt. B.3.3 auf S. 399)	Aktiviert	Aktiviert	Deaktiviert
Aktionen für infizierte Objekte (s. Pkt. B.3.5 auf S. 401)	Desinfizieren, löschen, wenn Desinfizieren nicht möglich ist	Desinfizieren, löschen, wenn Desinfizieren nicht möglich ist	Desinfizieren, löschen, wenn Desinfizieren nicht möglich ist
Aktion für verdächtige Objekte (s. Pkt. B.3.6 auf S. 403)	In Quarantäne verschieben	In Quarantäne verschieben	In Quarantäne verschieben
Objekte ausschließen (s. Pkt. B.3.8 auf S. 407)	Nein	Nein	Nein
Bedrohungen ausschließen (s. Pkt. B.3.9 auf S. 408)	Nein	Nein	Nein
Maximale Dauer der Objekt-Untersuchung (s. Pkt. B.3.10 auf S. 409)	60 Sek.	60 Sek.	60 Sek.
Maximale Größe des zu untersuchenden Compound-Objektes (s. Pkt. B.3.11 auf S. 410)	8 MB	Nein	Nein
Zusätzliche Ströme des Dateisystems (NTFS) untersuchen (s. Pkt. B.3.2 auf S. 397)	Ja	Ja	Ja
Bootsektoren untersuchen (s. Pkt. B.3.2 auf S. 397)	Ja	Ja	Ja

Parameter	**Sicherheitsstufe**		
	Maximales Tempo	**Empfohlen**	**Maximale Sicherheit**
Compound-Objekte untersuchen (s. Pkt. B.3.4 auf S. 400)	Gepackte Objekte* * Nur neue und veränderte	• SFX-Archive* • Gepackte Objekte* • Eingebettete OLE-Objekte* * Nur neue und veränderte	• SFX-Archive* • Gepackte Objekte* • Eingebettete OLE-Objekte* * Alle Objekte

Anmerkung

Beachten Sie, dass die Parameter für Sicherheit **Schutzmodus für Objekte**, **Übernahme von iChecker™** und **Übernahme von iSwift™** nicht zum Parametersatz der vordefinierten Sicherheitsstufen gehören. In der Grundeinstellung sind sie aktiviert. Wenn Sie nach der Entscheidung für eine vordefinierte Sicherheitsstufe den Status der Parameter für Sicherheit **Schutzmodus für Objekte**, **Übernahme von iChecker™** oder **Übernahme von iSwift™** ändern, bleibt die vordefinierte Sicherheitsstufe davon unberührt.

Um eine vordefinierte Sicherheitsstufe auszuwählen, machen Sie Folgendes:

1. In der Konsolenstruktur klappen Sie den Knoten **Echtzeitschutz** auf und gehen auf den eingebetteten Knoten **Echtzeitschutz für Dateien**.
2. Im Ergebnisfenster markieren Sie im Baum der File-Server-Ressourcen einen Knoten, für den Sie eine vordefinierte Sicherheitsstufe auswählen wollen.
3. Vergewissern Sie sich, dass dieser Knoten zum Schutzbereich gehört (s. Pkt. 6.2.1.3 auf S. 74).
4. Im Dialogfenster **Sicherheitsstufe** (s. Abbildung 19) wählen Sie die Sicherheitsstufe, die Sie übernehmen wollen, in der Liste **Sicherheitsstufe** aus.

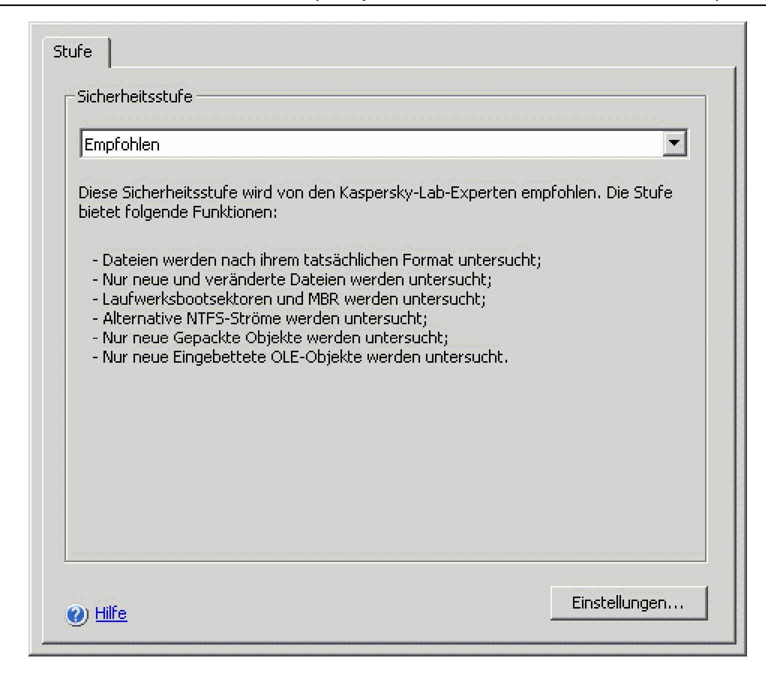


Abbildung 19. Dialogfenster **Sicherheitsstufe**

Im Dialogfenster wird die Liste der Parameterwerte für Sicherheit dargestellt, die der von Ihnen ausgewählten Sicherheitsstufe entsprechen.

5. Öffnen Sie das Kontextmenü mit einem Rechtsklick auf den Namen der Aufgabe und gehen Sie auf **Aufgabe speichern**, um die Änderungen in der Aufgabe zu speichern.

6.2.2.2. Parameter für Sicherheit von Hand einstellen

Standardmäßig werden in der Aufgabe **Echtzeitschutz für Dateien** die gleichen Parameter für Sicherheit angewendet wie für den gesamten Schutzbereich. Deren Werte entsprechen den Werten der vordefinierten Sicherheitsstufe **Empfohlen**. Die Parameterwerte für Sicherheit in der Grundeinstellung finden Sie in Pkt. 6.2.2.1 auf S. 79.

Sie können die standardmäßigen Parameterwerte für Sicherheit ändern, indem Sie sie für den gesamten Schutzbereich einheitlich oder für verschiedene Knoten im Baum der File-Server-Ressourcen unterschiedlich einstellen.

Die Parameter für Sicherheit, die Sie für einen ausgewählten Knoten einstellen können, werden automatisch für alle Knoten übernommen, die darin eingebettet sind. Wenn Sie jedoch die Parameter für Sicherheit eines eingebetteten Knoten separat einstellen, dann werden die Parameter für Sicherheit des übergeordneten Knoten für ihn nicht übernommen.

Um manuell die Parameter für Sicherheit eines ausgewählten Knotens einzustellen, machen Sie Folgendes:

1. In der Konsolenstruktur klappen Sie den Knoten **Echtzeitschutz** auf und gehen auf den eingebetteten Knoten **Echtzeitschutz für Dateien**.
2. Im Ergebnisfenster markieren Sie im Baum der File-Server-Ressourcen einen Knoten, dessen Parameter für Sicherheit Sie einstellen wollen.
3. Klicken Sie auf die Schaltfläche **Einstellung** im unteren Teil des Dialogfensters.

   Es öffnet sich das Dialogfenster **Parameter für Sicherheit**.

   > **Anmerkung**
   >
   > Wie die Vorlage Parameter für Sicherheit für einen Knoten angewendet wird, finden Sie in Pkt. 6.2.2.3 auf S. 86.

4. Konfigurieren Sie die Parameter für Sicherheit je nach Ihren Wünschen.
   - Auf der Registerkarte **Allgemein** (s. Abbildung 20) führen Sie die folgenden Aktionen aus:
     - Unter der Überschrift **Schutz von Objekten** bestimmen Sie, ob Anti-Virus alle Objekte des Schutzbereiches oder nur die Objekte mit bestimmten Formaten oder bestimmten Erweiterungen untersuchen soll, ob Anti-Virus die Boot-Sektoren und MBR, alternative NTFS-Datenströme untersuchen soll (s. Pkt. B.3.2 auf S. 397).
     - Legen Sie im Abschnitt **Optimierung** fest, ob Anti-Virus im gewählten Bereich alle Objekte untersuchen soll oder nur neue und veränderte Objekte (s. Pkt. B.3.3 auf S. 399);
     - Unter der Überschrift **Untersuchung von zusammengesetzten Objekten** geben Sie an, welche Compound-Objekte Anti-Virus untersuchen soll (s. Pkt. B.3.4 auf S. 400).

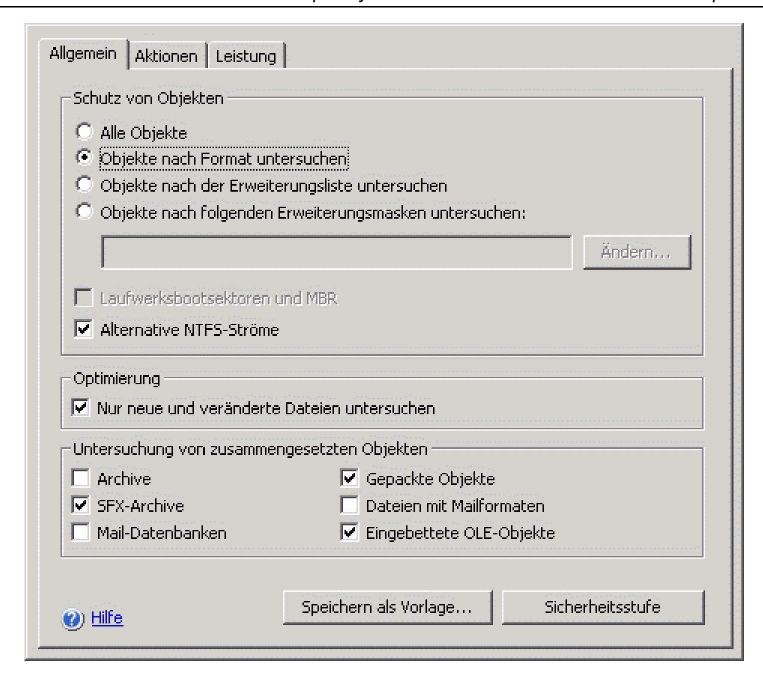


Abbildung 20. Dialogfenster **Parameter für Sicherheit**, Registerkarte **Allgemein**

- Auf der Registerkarte **Aktionen** (s. Abbildung 21) führen Sie die folgenden Aktionen aus:
  - Wählen Sie eine Aktion für infizierte Objekte aus (s. Pkt. B.3.5 auf S. 401).
  - Wählen Sie eine Aktion für verdächtige Objekte aus (s. Pkt. B.3.6 auf S. 403).
  - Bei Bedarf konfigurieren Sie die Aktionen für Objekte je nach Typ der im Objekt gefundenen Bedrohung (s. Pkt. B.3.7 auf S. 405).

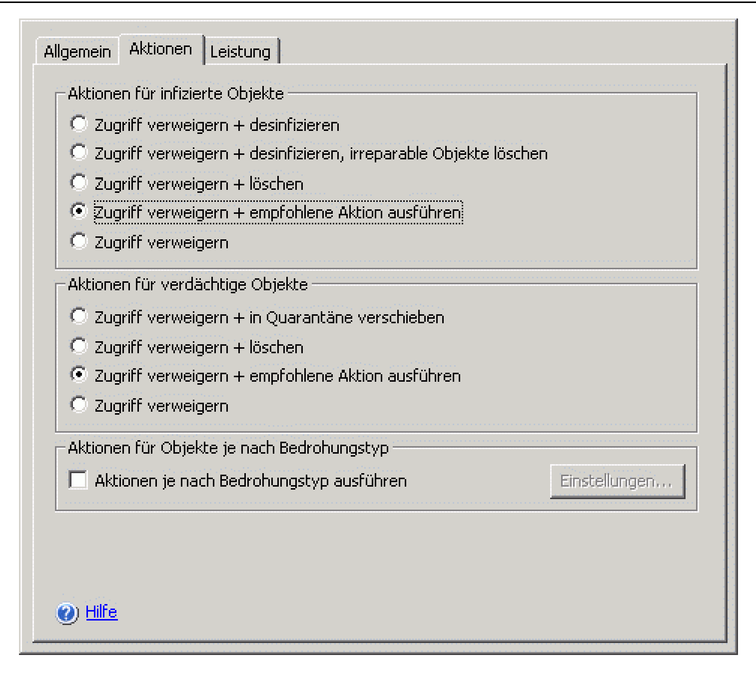


Abbildung 21. Dialogfenster **Parameter für Sicherheit**, Registerkarte **Aktionen**

- Auf der Registerkarte **Leistung** (s. Abbildung 22) führen Sie bei Bedarf die folgenden Aktionen aus:
  - Schließen Sie Dateien nach Name oder Maske aus (s. B.3.8 auf S. 407).
  - Schließen Sie Bedrohungen nach Name oder Namensmaske aus (s. Pkt. B.3.9 auf S. 408).
  - Geben Sie die maximale Dauer der Objekt-Untersuchung an (s. Pkt. B.3.10 auf S. 409).
  - Geben Sie die maximale Größe des zu untersuchenden Compound-Objektes an (s. Pkt. B.3.11 auf S. 410).
  - Aktivieren oder deaktivieren Sie die Übernahme von iChecker™ (s. Pkt. B.3.12 auf S. 410).
  - Aktivieren oder deaktivieren Sie die Übernahme von iSwift™ (s. Pkt. B.3.13 auf S. 411).

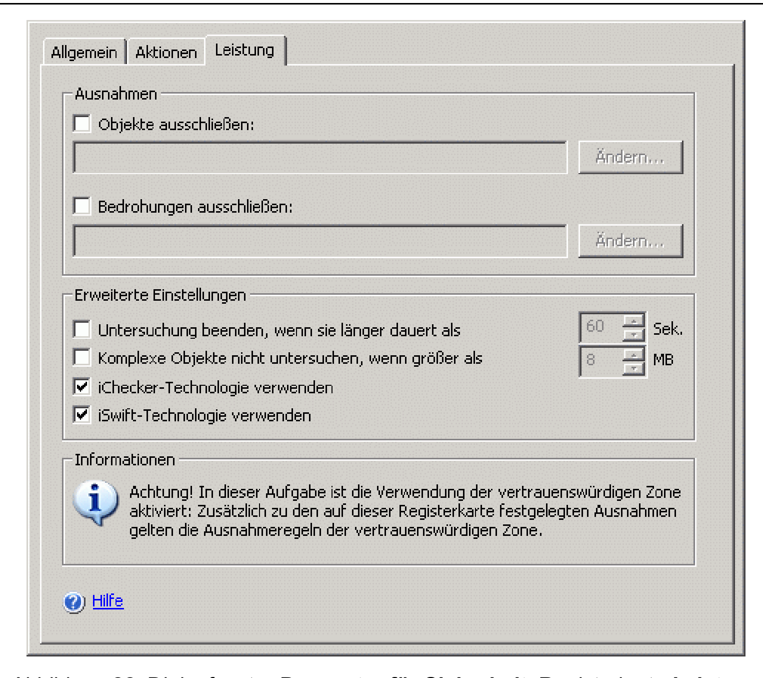


Abbildung 22. Dialogfenster **Parameter für Sicherheit**, Registerkarte **Leistung**

5. Nachdem Sie die gewünschten Parameter für Sicherheit eingestellt haben, öffnen Sie das Kontextmenü mit einem Rechtsklick auf den Namen der Aufgabe und gehen Sie auf **Speichern**, um die Änderungen an der Aufgabe zu speichern.

6.2.2.3. Vorlagen in der Aufgabe *Echtzeitschutz für Dateien*

In diesem Abschnitt stehen die folgenden Informationen:

- Speichern eines Parametersatzes für Sicherheit in Vorlage (s. Pkt. 6.2.2.3.1 auf S. 87)
- Parameter für Sicherheit in Vorlage anzeigen (s. Pkt. 6.2.2.3.2 auf S. 88)
- Übernehmen einer Vorlage (s. Pkt. 6.2.2.3.3 auf S. 89)
- Löschen einer Vorlage (s. Pkt. 6.2.2.3.4 auf S. 90)

6.2.2.3.1. Speichern eines Parametersatzes für Sicherheit in Vorlage

In der Aufgabe **Echtzeitschutz für Dateien** können Sie, nachdem Sie die Parameter für Sicherheit eines beliebigen Knotens im Baum der File-Server-Ressourcen eingestellt haben, diesen Parametersatz in einer Vorlage speichern, um sie später für einen anderen Knoten zu übernehmen.

Um einen Parametersatz für Sicherheit in einer Vorlage zu speichern, machen Sie Folgendes:

1. In der Konsolenstruktur klappen Sie den Knoten **Echtzeitschutz** auf und gehen auf den eingebetteten Knoten **Echtzeitschutz für Dateien**.
2. Im Ergebnisfenster markieren Sie im Baum der File-Server-Ressourcen einen Knoten, dessen Parameter für Sicherheit Sie speichern wollen.
3. Klicken Sie auf die Schaltfläche **Einstellung** im unteren Teil des Dialogfensters.
4. Im Dialogfenster **Parameter des Schutzbereichs** klicken Sie auf der Registerkarte **Allgemein** auf die Schaltfläche **Speichern als Vorlage**.
5. Im Dialogfenster **Eigenschaften der Vorlage** (s. Abbildung 23) machen Sie Folgendes:
   - Geben Sie im Feld **Vorlagenname** den Namen der Vorlage ein.
   - Im Feld **Beschreibung** tragen Sie beliebige Zusatzinformationen zur Vorlage ein.

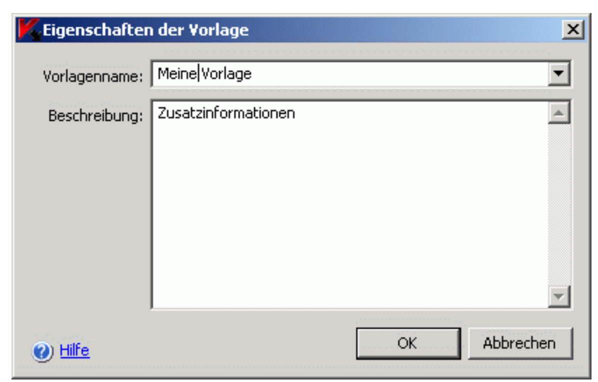


Abbildung 23. Dialogfenster **Eigenschaften der Vorlage**

6. Klicken Sie auf die Schaltfläche **OK**. Die Vorlage wird mit dem Parametersatz für Sicherheit gespeichert.

6.2.2.3.2. Parameter für Sicherheit in Vorlage speichern

Um die Werte der Parameter für Sicherheit in einer vorhandenen Vorlage anzuzeigen, machen Sie Folgendes:

1. In der Konsolenstruktur klappen Sie den Knoten **Echtzeitschutz** auf.
2. Öffnen Sie das Kontextmenü für die Aufgabe **Echtzeitschutz für Dateien** und gehen Sie auf den Eintrag **Vorlagen** (s. Abbildung 24).

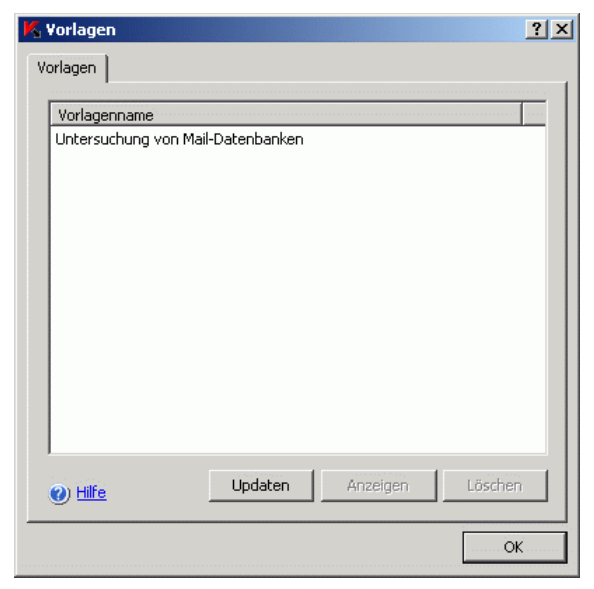


Abbildung 24. Dialogfenster **Vorlagen**

Im Dialogfenster **Vorlagen** steht eine Liste von Vorlagen, die Sie in der Aufgabe **Echtzeitschutz für Dateien** übernehmen können.

3. Um Daten über die Vorlage und die Parameterwerte anzuzeigen, markieren Sie die gewünschte Vorlage in der Liste und klicken Sie auf die Schaltfläche **Anzeigen** (s. Abbildung 25).

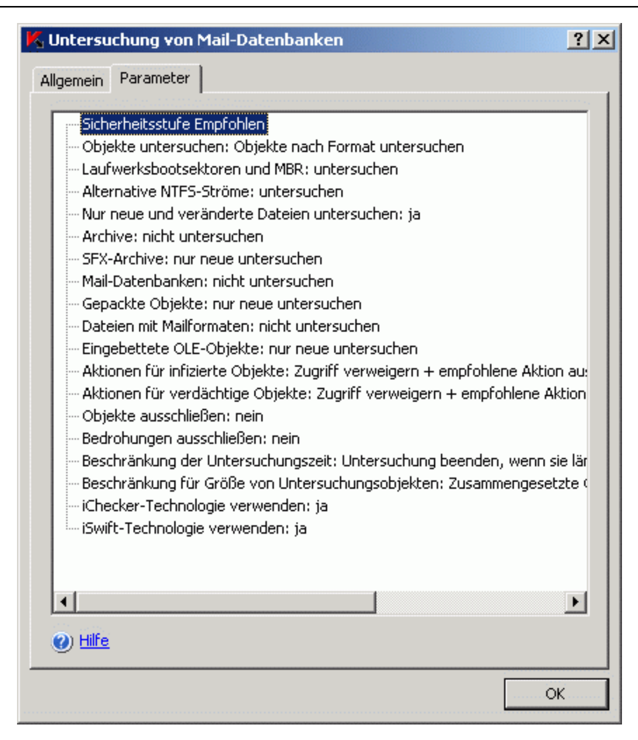


Abbildung 25. Dialogfenster **<Vorlagenname>**, Registerkarte **Parameter**

Auf der Registerkarte **Allgemein** werden der Name der Vorlage und zusätzliche Informationen über die Vorlage dargestellt. Auf der Registerkarte **Parameter** steht die Liste mit den Werten der Parameter für Sicherheit, die in der Vorlage gespeichert sind.

6.2.2.3.3. Vorlage übernehmen

Um eine Vorlage mit einem Satz von Parametern für Sicherheit eines ausgewählten Knotens zu übernehmen, machen Sie Folgendes:

1. Speichern Sie vorsichtshalber die Werte der Parameter für Sicherheit in einer Vorlage (s. Pkt. 6.2.2.3.1 auf S. 87).

2. In der Konsolenstruktur klappen Sie den Knoten **Echtzeitschutz** auf und gehen auf den eingebetteten Knoten **Echtzeitschutz für Dateien**.

3. Im Ergebnisfenster öffnen Sie im Baum der File-Server-Ressourcen das Kontextmenü für den Knoten, für den Sie eine Vorlage übernehmen wollen, und gehen Sie dann auf **Vorlage übernehmen**.

4. Im Dialogfenster **Vorlagen** wählen Sie die Vorlage aus, die Sie übernehmen wollen.

5. Öffnen Sie das Kontextmenü mit einem Rechtsklick auf den Namen der Aufgabe und gehen Sie auf **Aufgabe speichern**, um die Änderungen in der Aufgabe zu speichern.

Hinweis

Wenn Sie für einen übergeordneten Knoten eine Vorlage übernehmen, werden die Sicherheitsparameter der Vorlage auch für alle untergeordneten Knoten übernommen, unter Ausnahme jener, für welche die Sicherheitsparameter separat angepasst wurden.

Um die Sicherheitsparameter der Vorlage für alle untergeordneten Knoten zu übernehmen, deaktivieren Sie vor dem Übernehmen der Vorlage in der Struktur der Dateiressourcen des Servers das Kontrollkästchen des übergeordneten Knotens, und aktivieren Sie es anschließend wieder. Übernehmen Sie die Vorlage für den übergeordneten Knoten. Alle untergeordneten Knoten erhalten nun die gleichen Sicherheitsparameter wie der übergeordnete Knoten.

6.2.2.3.4. Vorlage löschen

Um eine Vorlage zu löschen, machen Sie Folgendes:

1. In der Konsolenstruktur klappen Sie den Knoten **Echtzeitschutz** auf.

2. Öffnen Sie das Kontextmenü für die Aufgabe **Echtzeitschutz für Dateien** und gehen Sie auf den Eintrag **Vorlagen** (s. Abbildung 24).

3. Im Dialogfenster **Vorlagen** markieren Sie in der Vorlagenliste die Vorlage, die Sie löschen wollen, und klicken Sie auf die Schaltfläche **Löschen**.

4. Im Dialogfenster zur Bestätigung klicken Sie auf die Schaltfläche **Ja**. Die ausgewählte Vorlage wird gelöscht.

6.2.3. Schutzmodus für Objekte auswählen

Sie können den Schutzmodus für Objekte in der Aufgabe **Echtzeitschutz für Dateien** auswählen. Details zum Parameter Schutzmodus finden Sie in Pkt. B.3.1 auf S. 396.

Um den Schutzmodus für Objekte auswählen, machen Sie Folgendes:

1. In der Konsolenstruktur klappen Sie den Knoten **Echtzeitschutz** auf.

2. Öffnen Sie das Kontextmenü für die Aufgabe **Echtzeitschutz für Dateien** und gehen Sie auf **Eigenschaften**.

3. Im Dialogfenster **Eigenschaften** markieren Sie auf der Registerkarte **Allgemein** (s. Abbildung 26) den Schutzmodus für Objekte, den Sie aktivieren wollen, und klicken Sie auf die Schaltfläche **OK**.

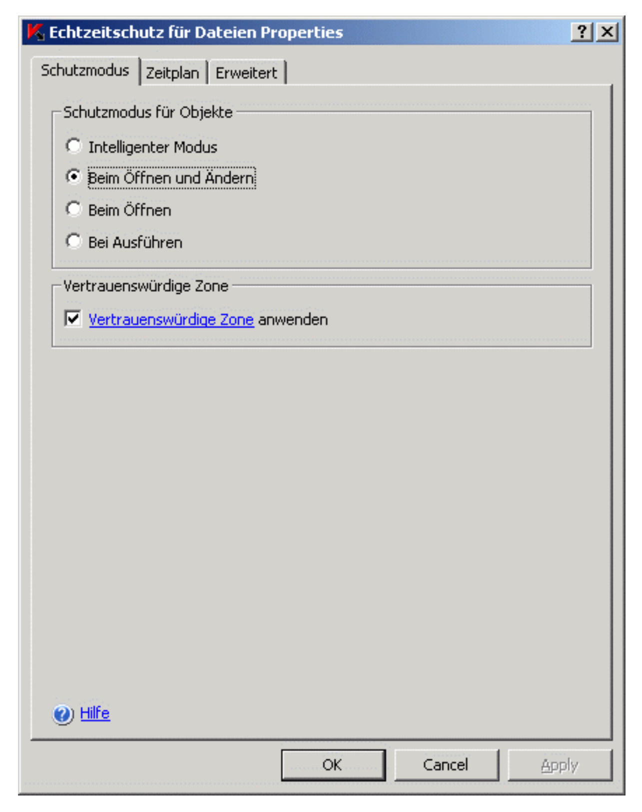


Abbildung 26. Dialogfenster **Eigenschaften der Aufgabe**, Registerkarte **Schutzmodus**

6.3. Statistik der Aufgabe *Echtzeitschutz für Dateien*

Solange die Aufgabe **Echtzeitschutz für Dateien** ausgeführt wird, können Sie Detailinformationen zur Anzahl der Objekte in Echtzeit anzeigen lassen, die Anti-Virus seit dem Aufgabenstart bis jetzt verarbeitet hat, eine so genannte *Statistik der Aufgabenausführung*.

*Um die Statistik für die Aufgabe **Echtzeitschutz für Dateien** anzuzeigen, machen Sie Folgendes:*

1. In der Konsolenstruktur klappen Sie den Knoten **Echtzeitschutz** auf.
2. Öffnen Sie das Kontextmenü für die Aufgabe **Echtzeitschutz für Dateien** und gehen Sie auf **Statistik**.

Im Dialogfenster **Statistik** werden die folgenden Angaben zu den Objekten angezeigt, die Anti-Virus seit dem Start der Aufgabe bis zum jetzigen Zeitpunkt verarbeitet hat.

Feld	Beschreibung
Gefundene Bedrohungen	Anzahl der erkannten Bedrohungen. Findet Anti-Virus beispielsweise in fünf Objekten ein Schadprogramm, dann wird der Wert in diesem Feld um eins erhöht
Gefundene infizierte Objekte	Summe der erkannten infizierten Objekte
Gefundene verdächtige Objekte	Summe der erkannten verdächtigen Objekte
Nicht desinfizierte Objekte	Anzahl der Objekte, die von Anti-Virus nicht desinfiziert wurden, weil: a) Bedrohungsart im Objekt kann nicht desinfiziert werden; b) Objekttyp kann nicht desinfiziert werden; c) beim Desinfizieren ist ein Fehler aufgetreten
Nicht in die Quarantäne verschobene Objekte	Anzahl der Objekte, die Anti-Virus repariert hat
Nicht gelöschte Objekte	Anzahl der Objekte, die Anti-Virus zu löschen versucht hat, was aber aus den folgenden Gründen fehlgeschlagen ist: Der Zugriff auf das Objekt ist von einem anderen Programm gesperrt
Nicht untersuchte Objekte	Anzahl der im Schutzbereich enthaltenen Objekte, deren Untersuchung durch Anti-Virus fehlgeschlagen ist, z.B. weil der Zugriff auf ein Objekt durch ein anderes Programm gesperrt war

Feld	Beschreibung
Nicht ins Backup verschobene Objekte	Anzahl der Objekte, die Anti-Virus zu löschen versucht hat, was aber fehlgeschlagen ist, weil beispielsweise der Zugriff auf das Objekt durch eine andere Anwendung gesperrt ist
Untersuchungsfehler	Anzahl der Dateien, deren Kopien Anti-Virus im Backup gespeichert hat
Desinfizierte Objekte	Anzahl der Dateien, deren Kopien Anti-Virus im Backup speichern wollte, was aber aufgrund eines Fehlers nicht gelungen ist
Nach Quarantäne verschoben	Anzahl der Objekte, die Anti-Virus in die Quarantäne verschoben hat
Ins Backup verschoben	Anzahl der Dateien, deren Kopien Anti-Virus im Backup gespeichert hat
Gelöschte Objekte	Erkannte Objekte, die Anti-Virus gelöscht hat
Kennwortgeschützte Objekte	Anzahl der Objekte (zum Beispiel Archive), die Anti-Virus übersprungen hat, weil diese Objekte mit einem Kennwort geschützt sind
Beschädigte Objekte	Summe der Objekte, die der Anti-Virus übersprungen hat, weil deren Format beschädigt war
Untersuchte Objekte	Summe der Objekte, die Anti-Virus untersucht hat

6.4. Aufgabe *Skript-Untersuchung* anpassen

Die Systemaufgabe **Skript-Untersuchung** besitzt in der Grundeinstellung die Parameter, die in Tabelle 4 beschrieben werden. Sie können die Werte dieser Parameter ändern und die Aufgabe anpassen.

Tabelle 4. Standardmäßige Parameter der Aufgabe *Skript-Untersuchung*

Parameter	Standardwert	Beschreibung
Ausführung infizierter Skripts	Verboten	Anti-Virus verbietet die Ausführung von Skripts, die als infiziert erkannt werden, immer.
Ausführung verdächtiger Skripts	Verboten	Sie können die Aktionen festlegen, die Anti-Virus mit Skripts ausführen soll, die als verdächtig erkannt werden: Ausführung verbieten oder erlauben.
Vertrauenswürdige Zone	Wird verwendet Liste der Ausnahmen ist leer	Einheitliche Liste mit Ausnahmen, die Sie in der Aufgabe **Skript-Untersuchung** verwenden können. Kapitel 8 auf S. 109 enthält Informationen über das Erstellen und die Verwendung der vertrauenswürdigen Zone.

*Um die Aufgabe **Skript-Untersuchung** anzupassen:*

1. Öffnen Sie in der Konsolenstruktur den Knoten **Echtzeitschutz**.
2. Öffnen Sie das Kontextmenü für die Aufgabe **Skript-Untersuchung** und wählen Sie den Befehl **Eigenschaften**.

   Das Dialogfenster **Eigenschaften: Skript-Untersuchung** wird geöffnet.
3. Erlauben oder verbieten Sie in der Parametergruppe **Aktionen für verdächtige Skripts** die Ausführung verdächtiger Skripts:
   - Um die Ausführung verdächtiger Skripts zu erlauben, wählen Sie **Ausführung erlauben**.
   - Um die Ausführung verdächtiger Skripts zu verbieten, wählen Sie **Ausführung sperren**.
4. Aktivieren oder deaktivieren Sie in der Parametergruppe **Vertrauenswürdige Zone** die Verwendung der vertrauenswürdigen Zone:
   - Um die Verwendung der vertrauenswürdigen Zone zu aktivieren, kreuzen Sie das Kontrollkästchen **Vertrauenswürdige Zone verwenden** an.
   - Um die Verwendung der vertrauenswürdigen Zone zu deaktivieren, entfernen Sie das Kontrollkästchen **Vertrauenswürdige Zone verwenden**.

Wie Skripts zur Liste der Ausnahmen der vertrauenswürdigen Zone hinzugefügt werden, wird in Pkt. 8.2.3 auf S. 116 beschrieben.

5. Klicken Sie im Dialogfenster **Eigenschaften: Skript-Untersuchung** auf **OK**, um die Änderungen zu speichern.

6.5. Statistik der Aufgabe *Skript-Untersuchung*

Solange die Aufgabe **Skript-Untersuchung** ausgeführt wird, können Sie Detail-informationen zur Anzahl der Skripte anzeigen lassen, die Anti-Virus seit dem Aufgabenstart bis jetzt verarbeitet hat, eine so genannte *Aufgabenstatistik*.

Um eine Aufgabe-Statistik anzuzeigen, machen Sie Folgendes:

1. In der Konsolenstruktur klappen Sie den Knoten **Echtzeitschutz** auf.
2. Öffnen Sie das Kontextmenü für die Aufgabe **Skript-Untersuchung** und gehen Sie auf **Statistik**.

Im Dialogfenster **Statistik** werden die folgenden Informationen angezeigt:

Feld	Beschreibung
Gesperrte Skripts	Anzahl der Skripte, deren Ausführung Anti-Virus unterbunden hat
Gefährliche Skripts	Anzahl der erkannten gefährlichen Skripte
Verdächtige Skripts	Anzahl der erkannten verdächtigen Skripte
Bearbeitete Skripts	Allgemeine Anzahl der verarbeiteten Skripte

KAPITEL 7. ZUGRIFFSSPERRE VON COMPUTERN IN DER AUFGABE ECHTZEITSCHUTZ FÜR DATEIEN

In diesem Kapitel stehen die folgenden Informationen:

7.1. Zugriff von Computern auf geschützten Server sperren

Wenn die Aufgabe **Echtzeitschutz für Dateien** ausgeführt wird, können Sie temporär den Zugriff von infizierten Computern auf den geschützten Server sperren.

Sie können den Zugriff von Rechnern auf zwei Wegen sperren:

- **Automatisch Zugriffssperre von Computern aktivieren**. Wenn ein Computer im Netzwerk versucht, infizierte oder verdächtige Objekte auf den geschützten Server zu schreiben, stuft Anti-Virus diesen Rechner als *infiziert* ein und führt die von Ihnen eingegebenen Aktionen aus: Er sperrt temporär den Zugriff des Rechners auf die Dateien des Servers und/oder startet eine von Ihnen angegebene ausführbare Datei. In der Grundeinstellung ist die automatische Zugriffssperre von Computern aktiviert.
- **Zugriff von infizierten Computern von Hand sperren**. Wenn Sie Informationen darüber haben, dass ein Computer im lokalen Netzwerk infiziert ist, dann können Sie diesem Computer den Zugang zum geschützten Server per Hand sperren: Fügen Sie den Rechner in die Sperrliste ein und geben Sie die Frist an, in der er auf die Objekte des geschützten Servers nicht zugreifen kann.

Sie können den Zugriff eines Computers auf den geschützten Server jederzeit freigeben.

Jeder Sperr- und Freigabevorgang für Computer wird im Bericht zum System-Audit registriert.

Die Liste mit den freigegebenen Computern wird automatisch zwischen den Anti-Virus-Instanzen gespeichert.

7.2. Automatisches Sperren des Zugriffs von Computern aktivieren oder deaktivieren

Um die Funktion Automatisches Sperren des Zugriffs von Computern zu aktivieren oder zu deaktivieren, machen Sie Folgendes:

1. In der Konsolenstruktur klappen Sie den Knoten **Echtzeitschutz** auf und gehen auf den Knoten **Echtzeitschutz für Dateien**, um den eingebetteten Knoten **Zugriff von Computern sperren** anzuzeigen.
2. Führen Sie eine der folgenden Aktionen aus:
   - Um das automatische Sperren des Zugriffs von Computern auf den Server zu aktivieren, klicken Sie mit der rechten Maustaste auf den Knoten **Zugriffsperre für Computer auf den Server** und wählen Sie den Befehl **Zugriffsperre für Computer auf den Server aktivieren**.

- Um das automatische Sperren des Zugriffs von Computern zu deaktivieren, klicken Sie mit der rechten Maustaste auf den Knoten **Zugriffsperre für Computer auf den Server** und wählen Sie den Befehl **Zugriffsperre für Computer auf den Server deaktivieren**.

3. Klicken Sie auf **OK**.

> **Hinweis**
>
> Wenn Sie die Funktion zur automatischen Zugriffssperre für Computer einschalten, wird sie nur dann ausgeführt, wenn die Aufgabe **Echtzeitschutz für Dateien** läuft.
>
> Sobald Sie die automatische Sperrfunktion deaktivieren, erhalten alle Computer der Liste Zugriff auf die Dateien des Servers.

7.3. Parameter automatische Zugriffsperre von Computern einstellen

In diesem Abschnitt wird beschrieben, wie die automatische Zugriffssperre von Computern auf den Server aktiviert und eingestellt wird. Die Parameter für Sperrungen werden in B.4 auf S. 413 näher beschrieben.

Um die Parameter für die automatische Zugriffssperre von Computern einzustellen, machen Sie Folgendes:

1. In der Konsolenstruktur klappen Sie den Knoten **Echtzeitschutz** auf und gehen auf den Knoten **Echtzeitschutz für Dateien**, um den eingebetteten Knoten **Zugriff von Computern sperren** anzuzeigen.

2. Öffnen Sie das Kontextmenü mit einem Rechtsklick auf den Knoten **Zugriff von Computern sperren** und gehen Sie auf **Eigenschaften**.

3. Im Dialogfenster **Eigenschaften: Zugriff von Computern sperren** auf der Registerkarte **Allgemein** vergewissern Sie sich, dass das Häkchen in **Zugriffssperre für Computer auf den Server aktivieren** gesetzt ist (s. Abbildung 27).

4. In der Parametergruppe **Aktionen mit dem Computer** aktivieren Sie Kontrollkästchen neben den Aktionen, die Anti-Virus ausführt, wenn von dem Computer aus versucht wird, ein infiziertes oder verdächtiges Objekt auf den Server zu schreiben (B.4.2 auf S. 414).

5. Wenn Sie **Zugriffssperre für Computer auf den Server aktivieren** gewählt haben, dann geben Sie die Zeitspanne an, für welche der Zugang zum Server gesperrt wird in Tagen, Stunden oder Minuten.

6. Wenn Sie **Ausführbare Datei starten** gewählt haben, dann klicken Sie auf die Schaltfläche ... und wählen Sie im Dialogfenster **Eigenschaften** (s. Abbildung 28) die ausführende Datei (Name und vollständiger Pfad zur Datei) sowie das Benutzerkonto, mit dessen Rechten die Datei ausgeführt werden soll.

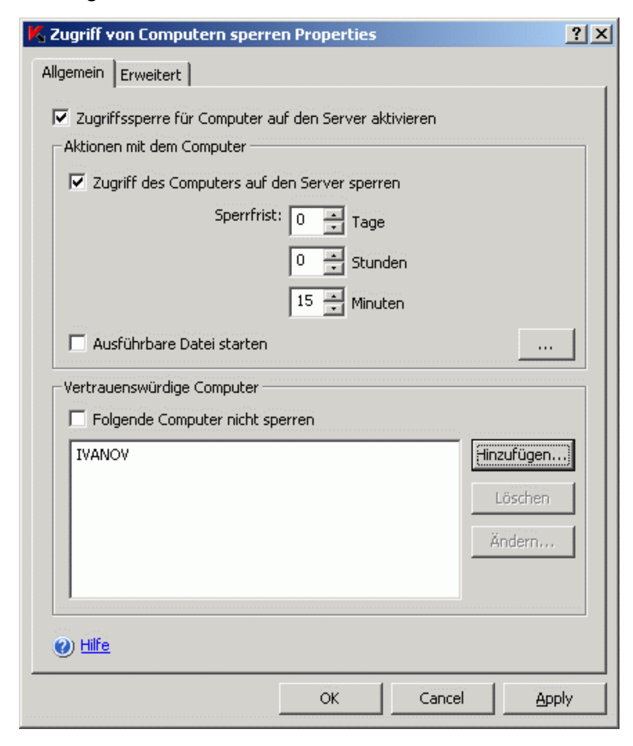


Abbildung 27. Dialogfenster **Eigenschaften: Zugriff von Computern sperren**, Registerkarte **Allgemein**

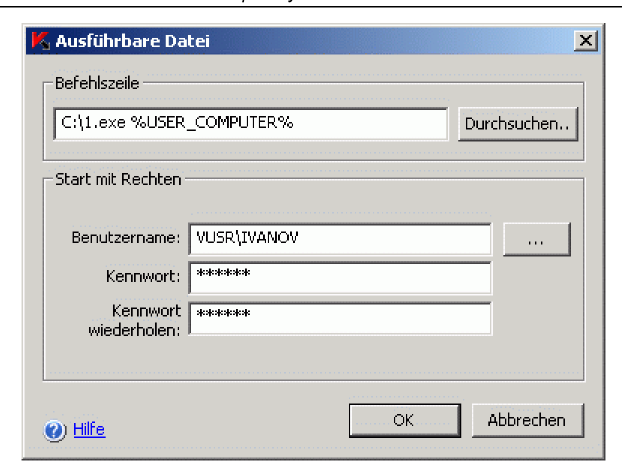


Abbildung 28. Dialogfenster **Ausführbare Datei**

7. Klicken Sie auf die Schaltfläche **OK**.

7.4. Computer von automatischer Sperre ausschließen (Vertrauenswürdige Computer)

Sie können eine Liste mit vertrauenswürdigen Computern anlegen (Details zum Parameter finden Sie in Pkt. B.4.3 auf S. 415).

Um einen Computer in die Liste Vertrauenswürdige Computer einzufügen, machen Sie Folgendes:

1. In der Konsolenstruktur klappen Sie den Knoten **Echtzeitschutz** auf und gehen auf den Knoten **Echtzeitschutz für Dateien**, um den eingebetteten Knoten **Zugriff von Computern sperren** anzuzeigen.

2. Öffnen Sie das Kontextmenü mit einem Rechtsklick auf den Knoten **Zugriff von Computern sperren** und gehen Sie auf **Eigenschaften**.

3. Im Dialogfenster **Eigenschaften: Zugriff von Computern sperren** auf der Registerkarte **Allgemein** (s. Abbildung 27) vergewissern Sie sich, dass das Häkchen in **Zugriffssperre für Computer auf den Server aktivieren** gesetzt ist (s. Pkt. B.4.1 auf S. 413).

4. In der Parametergruppe **Vertrauenswürdige Computer** setzen Sie das Häkchen in **Folgende Computer nicht sperren** und führen Sie folgende Aktionen durch:

   a) Klicken Sie auf die Schaltfläche **Hinzufügen**. Es öffnet sich das Dialogfenster Computer hinzufügen (s. Abbildung 29).

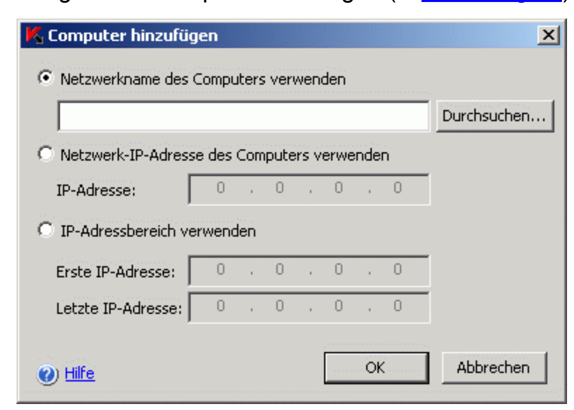


Abbildung 29. Dialogfenster **Computer hinzufügen**

   b) Geben Sie den Netzwerknamen oder die IP-Adresse des Computers an:

      - Wählen Sie **Netzwerkname des Computers verwenden** und geben Sie den NetBIOS-Namen des Computers an.
      - Geben Sie die statische IP-Adresse ein: Wählen Sie **Netzwerk-IP-Adresse des Computers verwenden** und geben Sie die IP-Adresse des Computers ein.
      - Geben Sie einen IP-Adressbereich ein: Wählen Sie **IP-Adressbereich verwenden**, tragen Sie den ersten IP-Adressbereich in das Feld **Erste IP-Adresse** und die letzte IP-Adresse in das Feld **Letzte IP-Adresse** ein. Alle Computer, welche zu diesem IP-Adressbereich gehören, werden als Vertrauenswürdige Computer behandelt;

   c) Klicken Sie auf die Schaltfläche **OK**.

5. Klicken Sie auf die Schaltfläche **OK** im Dialogfenster **Eigenschaften**.

7.5. Virenepidemien verhindern

In diesem Abschnitt wird beschrieben, wie das Verhindern von Virenepidemien aktiviert oder deaktiviert wird. Die Funktion *Virenepidemien verhindern* wird in Pkt. B.4.4 auf S. 416 näher beschrieben.

Um die Funktion Virenepidemien verhindern ein/auszuschalten, machen Sie Folgendes:

1. In der Konsolenstruktur klappen Sie den Knoten **Echtzeitschutz** auf und gehen auf den Knoten **Echtzeitschutz für Dateien**, um den eingebetteten Knoten **Zugriff von Computern sperren** anzuzeigen.
2. Öffnen Sie das Kontextmenü mit einem Rechtsklick auf den Knoten **Zugriff von Computern sperren** und gehen Sie auf **Eigenschaften**.
3. Im Dialogfenster **Eigenschaften: Zugriff von Computern sperren** öffnen Sie die Registerkarte **Erweitert** (s. Abbildung 30).

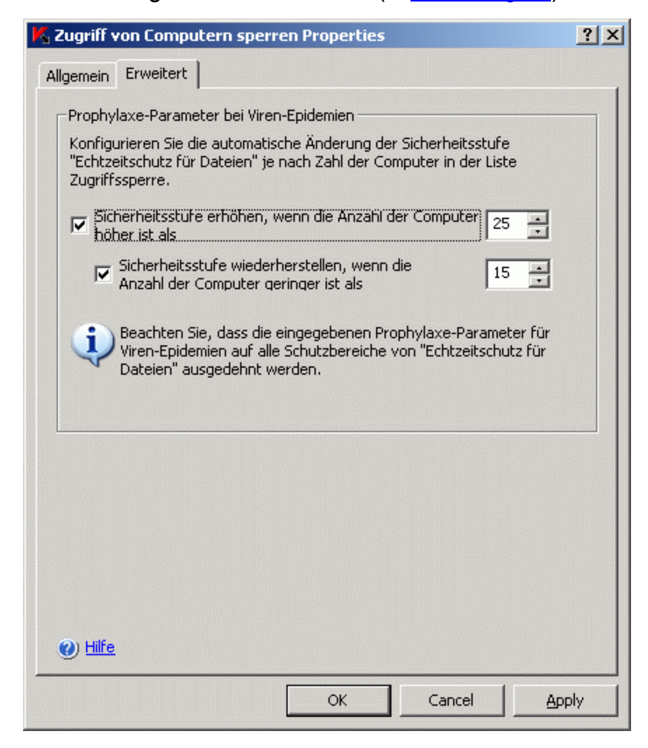


Abbildung 30. Dialogfenster **Eigenschaften: Zugriff von Computern sperren**, Registerkarte **Erweitert**

4. Auf der Registerkarte **Erweitert** führen Sie eine der folgenden Aktionen aus:

   - Um die Funktion Virenepidemien verhindern zu aktivieren, machen Sie Folgendes:

     a) Setzen Sie das Häkchen in **Sicherheitsstufe erhöhen, wenn die Anzahl der Computer höher ist als**.

     b) Geben Sie die Anzahl der Computer mit gesperrtem Zugriff an, die erreicht werden muss, damit Anti-Virus die Sicherheitsstufe hoch setzt.

     c) Bei Bedarf aktivieren Sie die Wiederherstellung der Sicherheitsstufe, wenn die Computer mit gesperrtem Zugriff bis auf den im Feld **Sicherheitsstufe wiederherstellen, wenn Anzahl der Computer geringer ist als** eingetragenen Wert sinkt.

   - Um die Funktion Virenepidemien verhindern abzuschalten, entfernen Sie das Häkchen in **Sicherheitsstufe erhöhen, wenn die Anzahl der Computer höher ist als**.

5. Klicken Sie auf die Schaltfläche **OK**.

7.6. Liste mit Computern anzeigen, deren Zugang auf den geschützten Server gesperrt ist

Achtung!

Computern in der Sperrliste wird der Zugang zum geschützten Server erst gesperrt, wenn die Aufgabe **Echtzeitschutz für Dateien** läuft und die Funktion automatische Zugriffssperre von Computern eingeschaltet ist.

Um die Computerliste anzuzeigen, für die der Zugang zum geschützten Server momentan gesperrt ist, machen Sie Folgendes:

1. In der Konsolenstruktur klappen Sie den Knoten **Echtzeitschutz** auf und gehen Sie dann auf den Knoten **Echtzeitschutz für** Dateien.

2. Öffnen Sie den eingebetteten Knoten **Zugriff von Computern sperren** (s. Abbildung 31).

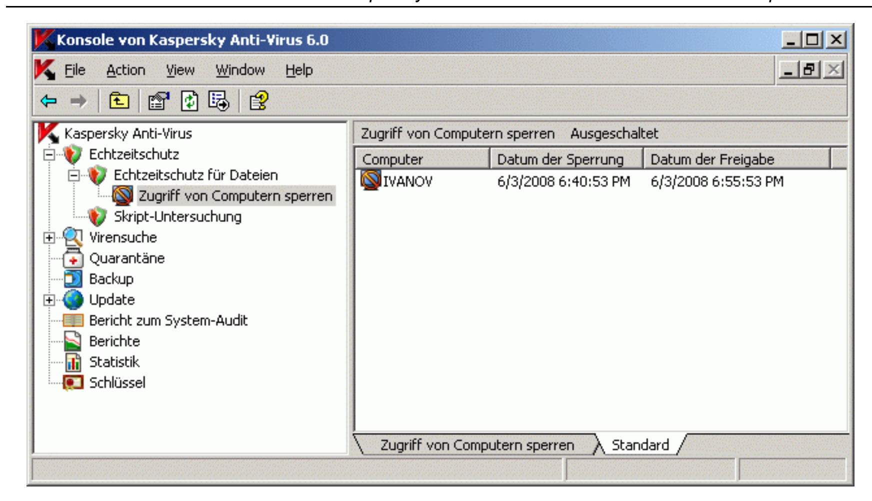


Abbildung 31. Fenster **Zugriff von Computern sperren**

Im Ergebnisfenster werden die folgenden Informationen zu Computern angezeigt, deren Zugriff auf den Server gesperrt ist:

Feld	Beschreibung
Computer	Informationen über den Computer in der Sperrliste. Diese Informationen wurden von Anti-Virus ermittelt (Netzwerkname, IP-Adresse des Computers)
Datum der Sperrung	Datum und Uhrzeit, wann der Zugang für den Computer gesperrt wurde; formatiert nach den Regionsoptionen von Microsoft Windows für den Computer, auf dem die Anti-Virus-Konsole installiert ist
Datum der Freigabe	Datum und Uhrzeit, wann der Zugang für den Computer gesperrt wird; formatiert nach den Regionsoptionen von Microsoft Windows für den Computer, auf dem die Anti-Virus-Konsole installiert ist

7.7. Zugriff von Computern von Hand sperren

Wenn Sie Informationen darüber haben, dass ein Computer im lokalen Netzwerk infiziert ist, dann können Sie für diesen Computer den Zugang zum geschützten Server per Hand sperren.

Achtung!

Computern in der Sperrliste wird der Zugang zum geschützten Server erst gesperrt, wenn die Aufgabe **Echtzeitschutz für Dateien** läuft und die Funktion automatische Zugriffssperre von Computern aktiviert ist.

Um den Zugang zum Server von einem Computer von Hand zu sperren, machen Sie Folgendes:

1. In der Konsolenstruktur klappen Sie den Knoten **Echtzeitschutz** auf und gehen Sie dann auf den Knoten **Echtzeitschutz für Dateien**.
2. Vergewissern Sie sich, dass die automatischen Zugriffssperre von Computern aktiviert ist (s. Pkt. 7.2 auf S. 97).
3. Öffnen Sie das Kontextmenü mit einem Rechtsklick auf den eingebetteten Knoten **Zugriff von Computern sperren** und gehen Sie auf **Zur Sperrliste hinzufügen**.
4. Im Dialogfenster **Computer in Sperrliste übernehmen** (s. Abbildung 32) geben Sie den Netzwerknamen des Computers an, für den der Zugang gesperrt werden soll.

Hinweis

Geben Sie im Feld **Computer** nur die Netzwerk-NetBIOS-Namen der Computer an, nicht die DNS-Adressen.

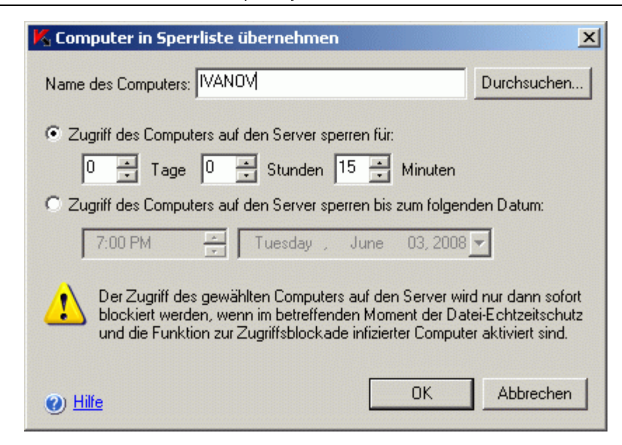


Abbildung 32. Dialogfenster **Zugriff eines Computers sperren**

5. Führen Sie eine der Aktionen durch:
   - Wählen Sie **Zugriff des Computers auf den Server sperren für** und geben Sie die Zeitperiode an, für die der Zugang des Computers zum Server gesperrt werden soll.
   - Wählen Sie **Zugriff des Computers auf den Server sperren bis zum folgenden Datum** und geben Sie Datum und Uhrzeit an, wann der Computer freigegeben werden soll.
6. Klicken Sie auf die Schaltfläche **OK**.

7.8. Zugriff von Computer freigeben

Sie können den Zugriff eines Computers auf den geschützten Server jederzeit freigeben.

Um den Zugriff von einem Computer freizugeben:

1. In der Konsolenstruktur klappen Sie den Knoten **Echtzeitschutz** auf und gehen Sie dann auf den Knoten **Echtzeitschutz für Dateien**.
2. Markieren Sie den eingebetteten Knoten **Zugriff von Computern sperren**.
3. Im Fenster **Zugriff von Computern sperren** klicken Sie in der Liste mit den gesperrten Computern mit der rechten Maustaste auf die Zeile, in der der Rechner steht, den Sie freigeben wollen, und wählen Sie dann **Zugriff von Computer zulassen** aus.

7.9. Statistik für Sperren anzeigen

Sie können Informationen über Rechner anzeigen, deren Zugriff auf den geschützten Server seit dem vergangenen Start des Anti-Virus gesperrt worden ist, die so genannte *Statistik für Sperrungen*.

Um die Statistik für Sperren anzuzeigen, machen Sie Folgendes:

1. In der Konsolenstruktur klappen Sie den Knoten **Echtzeitschutz** auf.
2. Klappen Sie den Knoten **Echtzeitschutz für Dateien** auf.
3. Öffnen Sie das Kontextmenü mit einem Rechtsklick auf den Knoten **Zugriff eines Computers sperren** und gehen Sie auf **Statistik** (s. Abbildung 33).

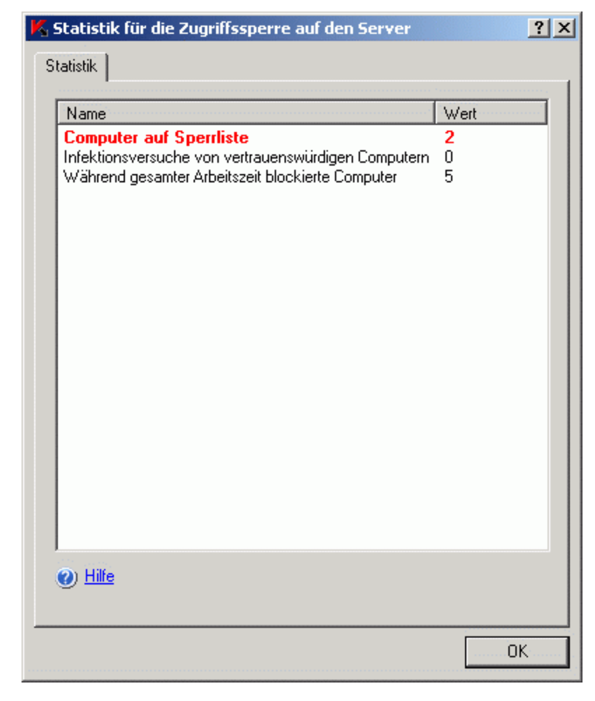


Abbildung 33. Dialogfenster **Statistik für die Zugriffssperre auf den Server**

Im Dialogfenster **Statistik für die Zugriffssperre auf den Server** werden die folgenden Informationen angezeigt:

Feld	Beschreibung
Computer auf Sperrliste	Aktuelle Menge an Computern in Sperrliste
Infektionsversuche von vertrauenswürdigen Computern	Menge der Versuche, infizierte oder verdächtige Objekte von vertrauenswürdigen Computern nach Aktivierung der automatischen Sperre auf den Server zu schreiben
Während gesamter Arbeitszeit blockierte Computer	Menge der Computer, die automatisch in die Sperrliste übernommen werden, wenn sie versuchen, infizierte oder verdächtige Objekte nach Aktivierung der automatischen Sperre auf den Server zu schreiben

KAPITEL 8. VERTRAUENSWÜRDIGE ZONE

Dieses Kapitel enthält folgende Informationen:

- Beschreibung der vertrauenswürdigen Zone von Anti-Virus (s. Pkt. 8.1 auf S. 109)
- Hinzufügen von Ausnahmen zur vertrauenswürdigen Zone (s. Pkt. 8.2 auf S. 111)
- Übernehmen der vertrauenswürdigen Zone (s. Pkt. 8.3 auf S. 120)

8.1. Über die vertrauenswürdige Zone von Anti-Virus

Sie können eine einheitliche Liste von Ausnahmen für den Schutzbereich (Untersuchungsbereich) anlegen. Diese Ausnahmen können bei Bedarf in ausgewählten Untersuchungsaufgaben und in der Aufgabe **Echtzeitschutz für Dateien** angewendet werden. Diese Liste von Ausnahmen heißt *vertrauenswürdige Zone*.

- Zur vertrauenswürdigen Zone von Anti-Virus können folgende Objekte gehören: Dateien, auf die Prozesse von Anwendungen zugreifen, die sensibel auf das Abfangen von Dateien reagieren (*vertrauenswürdige Prozesse*),
- Dateien, auf die im Verlauf von Backup-Operationen zugegriffen wird *(Backup-Operationen),*
- Objekte, die vom Benutzer durch ihren Ort und/oder durch eine Bedrohung darin festgelegt werden (*Regeln für Ausnahmen*).

Die vertrauenswürdige Zone wird standardmäßig in den Aufgaben **Echtzeitschutz für Dateien** und **Skript-Untersuchung**; in Systemaufgaben und in neu vom Benutzer erstellten Untersuchungsaufgaben verwendet.

Vertrauenswürdige Prozesse (wird nur in der Aufgabe **Echtzeitschutz für Dateien** verwendet)

Bestimmte Anwendungen auf dem Server können instabil arbeiten, wenn Dateien, auf die sie zugreifen, von der Antiviren-Anwendung abgefangen

werden. Zu diesen Anwendungen zählen beispielsweise Systemprogramme von Domain-Controllern.

Um die stabile Arbeit solcher Anwendungen zu gewährleisten, können Sie den Echtzeitschutz für jene Dateien deaktivieren, auf die die aktiven Prozesse dieser Anwendungen zugreifen. Dazu wird in der vertrauenswürdigen Zone eine Liste der vertrauenswürdigen Prozesse angelegt.

Die Firma Microsoft empfiehlt, bestimmte Anwendungen, die nicht infizierbar sind, vom Echtzeitschutz für Dateien auszuschließen. Eine Liste der Dateien, die als Ausnahmen empfohlen werden, finden Sie auf der Webseite der Firma Microsoft http://support.microsoft.com/kb/822158/de.

Die Funktion *Vertrauenswürdige Prozesse* kann aktiviert oder deaktiviert werden, wenn die vertrauenswürdige Zone übernommen wird.

Beachten Sie, dass Anti-Virus einen Prozess aus der vertrauenswürdigen Liste löscht, wenn seine ausführbare Datei beispielsweise durch ein Update verändert wird.

Backup-Operationen (wird nur in der Aufgabe **Echtzeitschutz für Dateien** verwendet)

Sie können den Echtzeitschutz für Dateien, auf die bei Operationen zum Sicherungskopieren zugegriffen wird, während dem Anlegen von Sicherungskopien abschalten. Anti-Virus untersucht Dateien nicht, die von einem Backup-Programm mit dem Attribut FILE_FLAG_BACKUP_SEMANTICS zum Lesen geöffnet werden.

Die Funktion zum Abschalten des Echtzeitschutzes für Dateien während Backup-Operationen kann aktiviert oder deaktiviert werden, wenn die vertrauenswürdige Zone übernommen wird.

Regeln für Ausnahmen (wird in den Aufgaben **Echtzeitschutz für Dateien** und **Skript-Untersuchung** und in den Aufgaben zur Virensuche verwendet)

Sie können Objekte in einzelnen Aufgaben ausschließen, die vertrauenwwürdige Zone nicht verwenden, oder Sie können eine einheitliche Liste von mit Ausnahmen in der der vertrauenswürdigen Zone speichern und diese Ausnahmen bei Bedarf in bestimmten Aufgaben verwenden: **Echtzeitschutz für Dateien**, **Skript-Untersuchung** oder Aufgaben zur Virensuche.

Sie können der vertrauenswürdigen Zone Objekte hinzufügen, die durch den Pfad auf dem Server, durch den Namen der in ihnen Objekt gefundenen Bedrohung oder durch eine Kombination dieser Merkmale angegeben wird.

Wenn Sie der vertrauenswürdigen Zone eine neue Ausnahme hinzufügen, legen sie eine Regel dafür fest (Merkmale, nach denen Anti-Virus Objekte überspringen soll) und bestimmen, für welche Aufgaben (**Echtzeitschutz für Dateien**, **Skript-Untersuchung** und/oder **Virensuche**) die Regel gelten soll.

Entsprechend der von Ihnen erstellten Regel, kann Anti-Virus in den Aufgaben der festgelegten Komponenten folgende Objekte überspringen:

- festgelegte Bedrohungen in bestimmten Serverbereichen
- alle Bedrohungen in bestimmten Serverbereichen
- festgelegte Bedrohungen im gesamten Untersuchungsbereich

Wenn Sie bei der Installation von Anti-Virus die Optionen **Bedrohungen nach Maske not-a-virus:RemoteAdmin* zu Ausnahmen hinzufügen** und **Dateien zu Ausnahmen hinzufügen, die Microsoft empfiehlt** gewählt haben, werden die Ausnahmeregeln in der Aufgabe **Echtzeitschutz für Dateien** sowie in Systemaufgaben zur Virensuche verwendet, unter Ausnahme der Aufgaben **Untersuchung von Quarantäne-Objekten** und **Integritätskontrolle für Anwendungen**.

8.2. Ausnahmen zur vertrauenswürdigen Zone hinzufügen

Dieser Abschnitt enthält folgende Informationen:

- Hinzufügen von Prozessen zur Liste der vertrauenswürdigen Prozesse (s. Pkt. 8.2.1 auf S. 111)
- Deaktivieren des Echtzeitschutzes für Dateien während dem Anlegen von Sicherungskopien (s. Pkt. 8.2.2 auf S. 115)
- Hinzufügen von Regeln für Ausnahmen (s. Pkt. 8.2.3 auf S. 116)

8.2.1. Prozesse zur vertrauenswürdigen Liste hinzufügen

Um die Arbeit von Anwendungen, die im Hinblick auf das Abfangen von Dateien sensibel sind, nicht zu stören, können Sie den Echtzeitschutz für Dateien deaktivieren, auf die die aktiven Prozesse dieser Anwendungen zugreifen. Dazu wird in der vertrauenswürdigen Zone eine Liste der vertrauenswürdigen Prozesse angelegt.

Ein Prozess kann der vertrauenswürdigen Liste auf zwei Arten hinzugefügt werden:

- Den Prozess aus der Liste der Prozesse auswählen, die im Augenblick auf dem geschützten Server aktiv sind.
- Die ausführbare Datei des Prozesses auswählen, unabhängig davon, ob der Prozess gerade aktiv ist oder nicht.

Hinweis

Wenn die ausführbare Datei eines Prozesses verändert wird, löscht Anti-Virus den Prozess aus der vertrauenswürdigen Liste.

Um einen Prozess zur vertrauenswürdigen Liste hinzuzufügen:

1. Öffnen Sie in der Anti-Virus-MMC-Konsole das Kontextmenü für den Namen des Anti-Virus-Snap-Ins und wählen Sie den Befehl **Vertrauenswürdige Zone einstellen**.
2. Aktivieren Sie im Dialogfenster **Vertrauenswürdige Zone** auf der Registerkarte **Vertrauenswürdige Prozesse** (s. Abbildung 34) die Funktion V*ertrauenswürdige Prozesse*, indem Sie das Kontrollkästchen **Datei-Aktivität der angegebenen Prozesse nicht untersuchen** aktivieren.

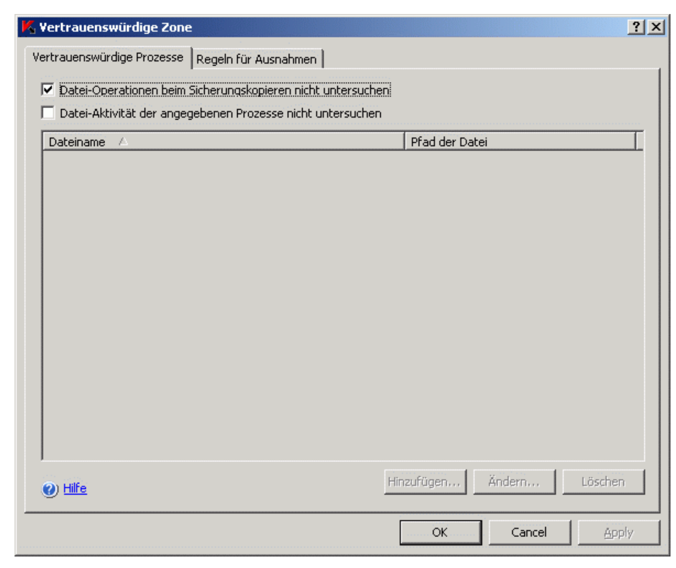


Abbildung 34. Dialogfenster **Vertrauenswürdige Zone,** Registerkarte **Vertrauenswürdige Prozesse**

3. Fügen Sie den vertrauenswürdigen Prozess aus der Liste der ausführbaren Prozesse hinzu und geben Sie die ausführbare Datei des Prozesses an.

- Um einen Prozess aus der Liste der aktiven Prozesse hinzuzufügen:
  a) Klicken Sie auf die Schaltfläche **Hinzufügen**.
  b) Klicken Sie im Dialogfenster **Vertrauenswürdigen Prozess hinzufügen** (s. Abbildung 35) auf die Schaltfläche **Prozesse**.

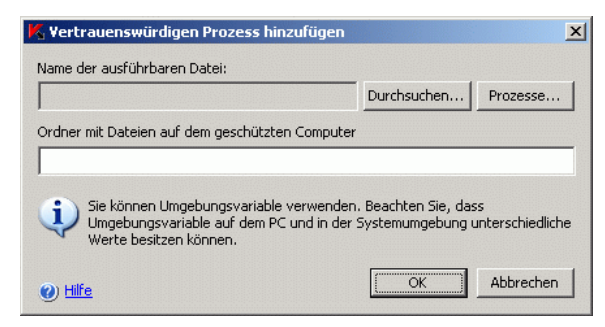


Abbildung 35. Dialogfenster **Vertrauenswürdigen Prozess hinzufügen**

  c) Wählen Sie im Dialogfenster **Aktive Prozesse** (s. Abbildung 36) den betreffenden Prozess aus und klicken Sie auf **OK**.

  Um den gewünschten Prozess in der Liste zu suchen, können Sie die Prozesse nach Namen, PID oder Pfad der ausführbaren Prozessdatei anordnen.

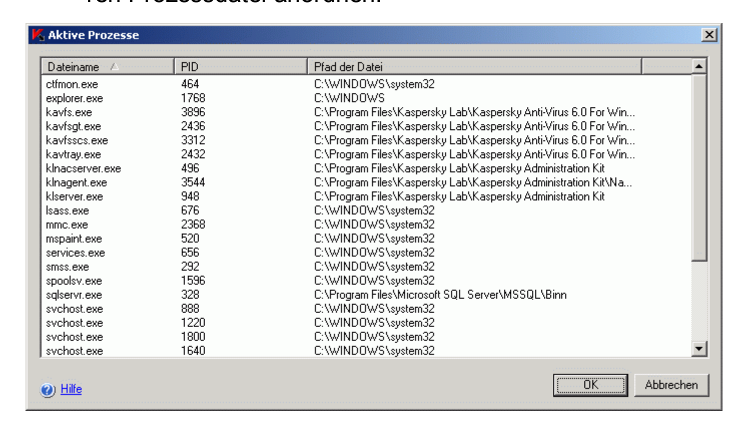


Abbildung 36. Dialogfenster **Aktive Prozesse**

> **Hinweis**
>
> Um die auf dem Server aktiven Prozesse anzuzeigen, müssen Sie zur Gruppe der lokalen Administratoren auf dem geschützten Server gehören.

Der gewählte Prozess wird im Dialogfenster **Vertrauenswürdige Prozesse** zur Liste der vertrauenswürdigen Prozesse hinzugefügt.

- Um die ausführbare Datei eines Prozesses auf einem Laufwerk des geschützten Servers auszuwählen, gehen Sie folgendermaßen vor:

  a) Klicken Sie auf der Registerkarte **Vertrauenswürdige Prozesse** auf die Schaltfläche **Hinzufügen**.

  b) Klicken Sie im Dialogfenster **Vertrauenswürdigen Prozess hinzufügen** auf die Schaltfläche **Durchsuchen** und wählen Sie die ausführbare Datei des Prozesses auf einem Laufwerk des geschützten Servers aus. Klicken Sie auf **OK**.

  Im Dialogfenster **Vertrauenswürdigen Prozess hinzufügen** werden der Name und der Pfad der Datei angezeigt.

  Wenn Sie die Pfade angeben, können Sie die Umgebungsvariablen des Systems verwenden. Dagegen können Sie die benutzerdefinierten Umgebungsvariablen nicht verwenden.

  > **Hinweis**
  >
  > Anti-Virus betrachtet einen Prozess nicht als vertrauenswürdig, wenn sich der Pfad der ausführbaren Prozessdatei von dem Pfad unterscheidet, den Sie im Feld **Pfad der Datei** angegeben haben. Wenn Sie möchten, dass der Prozess unabhängig davon, an welchem Ort sich die Datei befindet, aus der der Prozess gestartet wird, als vertrauenswürdig gilt, dann geben Sie im Feld **Pfad der Datei** das Zeichen ***** an. Bei der Pfadangabe können Umgebungsvariable verwendet werden.

  c) Klicken Sie auf **OK**.

  Der Name der ausgewählten ausführbaren Prozessdatei wird auf der Registerkarte **Vertrauenswürdige Prozess** in der Liste der vertrauenswürdigen Prozesse angezeigt.

4. Klicken Sie auf **OK**, um die Änderungen zu speichern.

5. Vergewissern Sie sich, dass die vertrauenswürdige Zone auf der Registerkarte **Echtzeitschutz für Dateien** (s. Pkt. 8.3 auf S. 120) übernommen wird.

8.2.2. Echtzeitschutz für Dateien während Backup-Operationen deaktivieren

Sie können den Echtzeitschutz für Dateien, auf die bei Operationen zum Sicherungskopieren zugegriffen wird, während dem Anlegen von Sicherungskopien deaktivieren. Anti-Virus untersucht Dateien nicht, die von einem Backup-Programm mit dem Attribut FILE_FLAG_BACKUP_SEMANTICS zum Lesen geöffnet werden.

> **Hinweis**
>
> Angaben zu der Anzahl der Dateien, die Anti-Virus bei Operationen zum Sicherungskopieren übersprungen hat, werden nicht im Dialogfenster **Statistik** der Aufgabe **Echtzeitschutz für Dateien** angezeigt.

Um den Echtzeitschutz für Dateien bei Backup-Operationen auszuschalten:

1. Öffnen Sie in der Anti-Virus-Konsole in der MMC das Kontextmenü für den Namen des Anti-Virus-Snap-Ins und wählen Sie den Befehl **Vertrauenswürdige Zone einstellen**.
2. Nehmen Sie im Dialogfenster **Vertrauenswürdige Zone** auf der Registerkarte **Vertrauenswürdige Prozesse** eine der folgenden Aktionen vor:
   - Um den Echtzeitschutz für Dateien, auf die in einer Backup-Aufgabe zugegriffen wird, auszuschalten, aktivieren Sie das Kontrollkästchen **Datei-Operationen beim Sicherungskopieren nicht untersuchen**.
   - Um den Echtzeitschutz für Dateien, auf die in einer Backup-Aufgabe zugegriffen wird, einzuschalten, deaktivieren Sie das Kontrollkästchen **Datei-Operationen beim Sicherungskopieren nicht untersuchen**.
3. Klicken Sie auf **OK**, um die Änderungen zu speichern.
4. Vergewissern Sie sich, dass die vertrauenswürdige Zone auf der Registerkarte **Echtzeitschutz für Dateien** (s. Pkt. 8.3 auf S. 120) übernommen wird.

8.2.3. Ausnahmeregeln hinzufügen

Um eine Regel für Ausnahmen hinzuzufügen:

1. Öffnen Sie in der Anti-Virus-Konsole in der MMC das Kontextmenü für den Namen des Anti-Virus-Snap-Ins und wählen Sie den Befehl **Vertrauenswürdige Zone einstellen**.
2. Klicken Sie im Dialogfenster **Vertrauenswürdige Zone** auf der Registerkarte **Regeln für Ausnahmen** auf die Schaltfläche **Hinzufügen**.

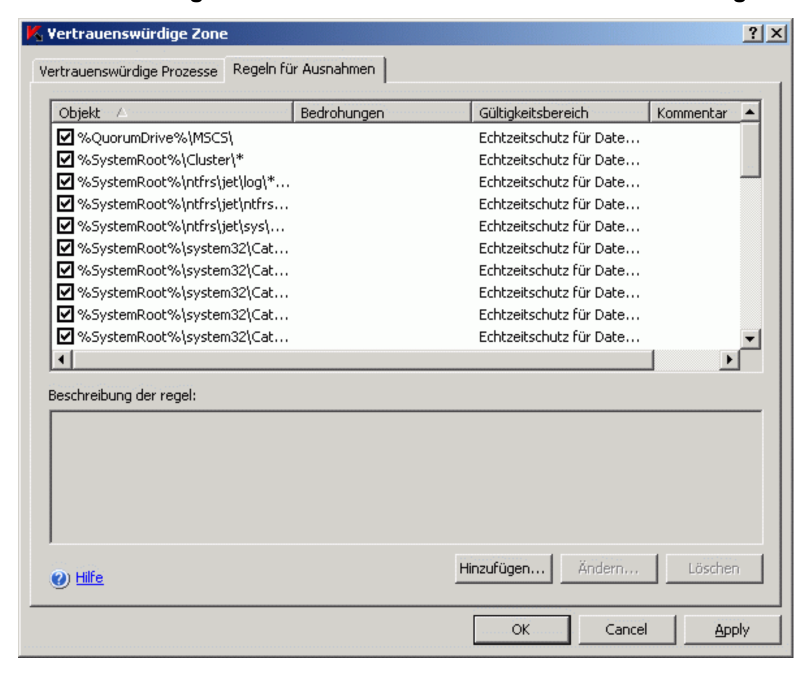


Abbildung 37. Dialogfenster **Vertrauenswürdige Zone**, Registerkarte **Regeln für Ausnahmen**

Das Dialogfenster **Ausnahmeregel** wird geöffnet.

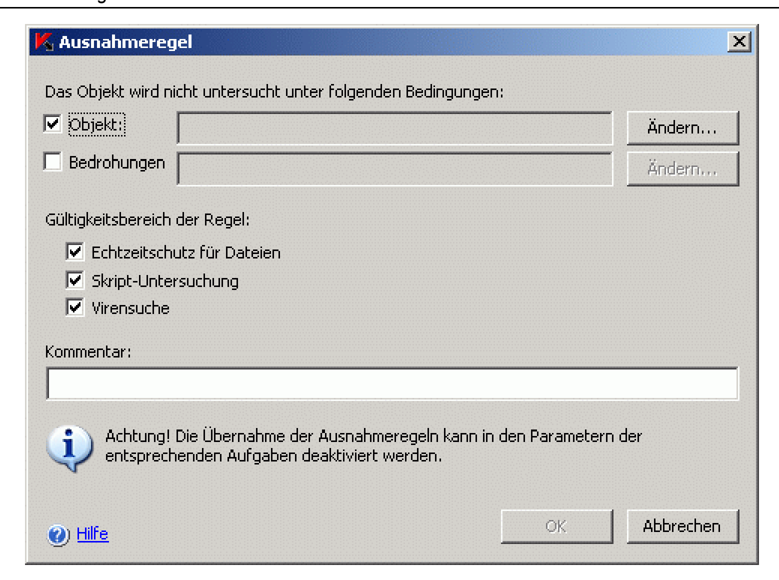


Abbildung 38. Dialogfenster **Ausnahmeregel**

3. Geben Sie die Regel an, nach der Anti-Virus das Objekt ausschließen soll.

Hinweis

Um *festgelegte Bedrohungen in bestimmten Bereichen* auszuschließen, aktivieren Sie die Kontrollkästchen **Objekt** und **Bedrohungen**.

Um *alle Bedrohungen in bestimmten Serverbereichen* auszuschließen, aktivieren Sie das Kontrollkästchen **Objekt** und deaktivieren Sie das Kontrollkästchen **Bedrohungen**.

Um festgelegte *Bedrohungen im gesamten Untersuchungsbereich* auszuschließen, deaktivieren Sie das Kontrollkästchen **Objekt** und aktivieren Sie das Kontrollkästchen.

- *Wenn Sie den Pfad des Objekts festlegen möchten,* aktivieren Sie das Kontrollkästchen **Objekt**, klicken Sie auf **Ändern**, geben Sie im Dialogfenster **Objekt wählen** (s. Abbildung 39) den Typ der Objekte an, der von der Untersuchung ausgeschlossen werden soll, und klicken Sie anschließend auf **OK**:
  - **Vordefinierter Bereich**. Wählen Sie einen vordefinierten Untersuchungsbereich aus der Liste aus.

- **Laufwerk oder Ordner**. Geben Sie ein Serverlaufwerk oder einen Ordner auf dem Server oder im lokalen Netzwerk an.
- **Datei**. Geben Sie eine Datei auf dem Server oder im lokalen Netzwerk an.
- **Datei oder URL-Adresse eines Skripts**. Geben Sie ein Skript auf dem geschützten Server, im lokalen Netzwerk oder im Internet an.

Hinweis

Bei der Angabe von Masken für die Namen von Objekten können die Zeichen ? und * verwendet werden.

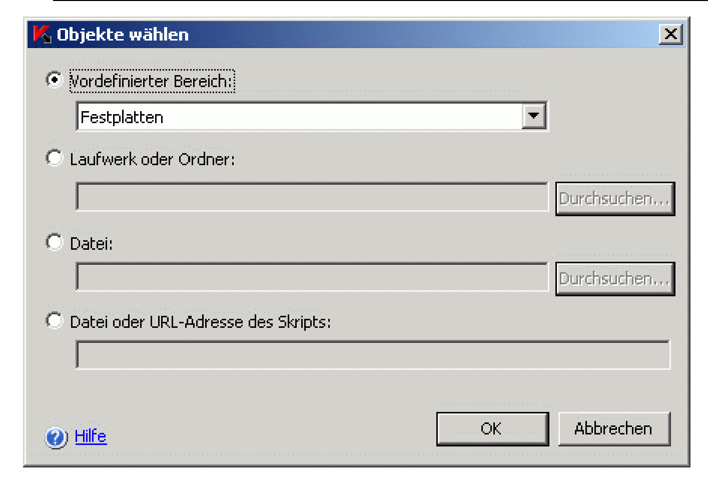


Abbildung 39. Dialogfenster **Objekt wählen**

- *Wenn Sie den Namen einer Bedrohung festlegen möchten*, klicken Sie auf **Ändern** und fügen Sie im Dialogfenster **Liste der Ausnahmen** (s. Abbildung 40) den Namen der Bedrohung hinzu (Details zu diesem Parameter finden Sie in Pkt. B.3.9 auf S. 408).

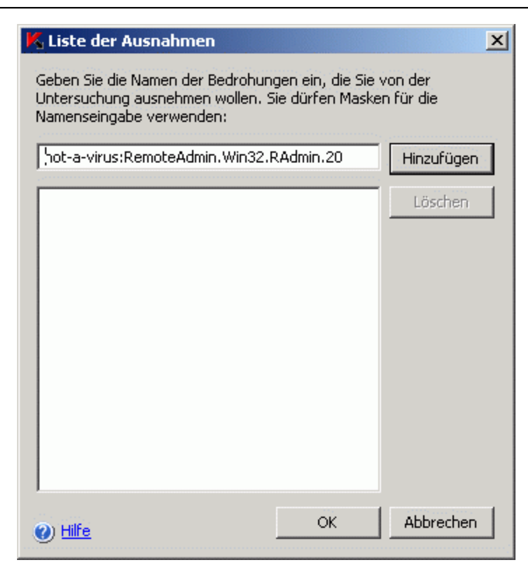


Abbildung 40. Dialogfenster **Liste der Ausnahmen**

4. Im Dialogfenster **Ausnahmeregel** unter der Überschrift **Gültigkeitsbereich der Regel** aktivieren Sie die Kontrollkästchen neben den Namen der funktionalen Komponenten, in deren Aufgaben die Ausnahmeregel übernommen werden soll.

5. Klicken Sie auf **OK**.

   - Um eine Regel anzupassen, wählen Sie die betreffende Regel im Dialogfenster **Vertrauenswürdige Zone** auf der Registerkarte **Regeln für Ausnahmen** aus, klicken Sie auf **Ändern** und nehmen Sie im Dialogfenster **Ausnahmeregel** die entsprechenden Änderungen vor.

   - Um eine Regel zu löschen, wählen Sie die betreffende Regel im Dialogfenster **Vertrauenswürdige Zone** auf der Registerkarte **Regeln für Ausnahmen** aus, klicken Sie auf **Löschen** und bestätigen Sie die Operation.

6. Klicken Sie im Dialogfenster **Vertrauenswürdige Zone** auf **OK**.

8.3. Vertrauenswürdige Zone übernehmen

Die vertrauenswürdige Zone wird standardmäßig in den Aufgaben der Komponente **Echtzeitschutz**, in Systemaufgaben und in neu erstellten Untersuchungsaufgaben übernommen.

Im Dialogfenster **Eigenschaften: <Aufgabe>** können Sie das Übernehmen der vertrauenswürdigen Zone in den einzelnen Aufgaben aktivieren oder deaktivieren.

Nachdem die vertrauenswürdige Zone aktiviert bzw. deaktiviert wurde, werden die Ausnahmen je nach Aufgabe zu unterschiedlichen Zeitpunkten wirksam bzw. unwirksam: in der Aufgabe **Echtzeitschutz für Dateien** und **Skript-Untersuchung** sofort, in Aufgaben zur Virensuche beim nächsten Start der Aufgabe.

Um die Ausnahmen der vertrauenswürdigen Zone in einer Aufgabe zu übernehmen:

1. Öffnen Sie auf der Anti-Virus-Konsole in der MMC das Kontextmenü für den Namen der Aufgabe und aktivieren Sie im Dialogfenster **Eigenschaften: <Aufgabe>** auf der Registerkarte **Allgemein** das Kontrollkästchen **Vertrauenswürdige Zone anwenden.**
2. Klicken Sie auf **OK**.

KAPITEL 9. VIRENSUCHE

In diesem Kapitel stehen die folgenden Informationen:

- Aufgaben zur Virensuche (s. Pkt. 9.1 auf S. 121)
- Einstellung für Aufgaben zur Virensuche (s. 9.2 auf S. 122)
- Aufgaben zur Virensuche im Hintergrund (s. 9.3 auf S. 143)
- Statistik für Aufgaben zur Virensuche (s. 9.4 auf S. 146)

9.1. Aufgaben zur Virensuche

Im Anti-Virus sind vier Systemaufgaben zur Virensuche vorgesehen:

- Die Aufgabe **Vollständige Untersuchung des Computers** wird wöchentlich nach Zeitplan ausgeführt. Anti-Virus untersucht alle Objekte des geschützten Servers mit Parametern für Sicherheit, deren Werte der Stufe **Empfohlen** entsprechen (s. Pkt. 9.2.2.1 auf S. 132). Sie können die Parameter für die Aufgabe **Vollständige Untersuchung des Computers** ändern.
- Die Aufgabe **Untersuchung von Quarantäne-Objekten** wird nach jedem Update der Datenbanken nach Zeitplan ausgeführt. Anti-Virus untersucht den Quarantäne-Ordner mit Parametern, die in Pkt. 11.3 auf S. 175 stehen. Sie können die Parameter für die Aufgabe **Untersuchung von Quarantäne-Objekten** nicht ändern.
- Die Aufgabe **Untersuchung bei Systemstart** wird nach Zeitplan bei jedem Start des Servers ausgeführt. Anti-Virus untersucht die Objekte des Autostarts, seine eigenen Programm-Module, die Boot-Sektoren und Master Boot Sektoren der Festplatten und Wechseldatenträger, den Arbeits- und den Prozessspeicher. Anti-Virus übernimmt die vordefinierte Sicherheitsstufe **Empfohlen** (s. Pkt. 9.2.2.1 auf S. 132). Sie können den Zeitplan der Aufgabe ändern oder den durch Zeitplan gesteuerten Start der Aufgabe deaktivieren.
- Die Aufgabe **Integritätskontrolle für Anwendungen** wird nach Zeitplan beim Start des Anti-Virus ausgeführt. Anti-Virus untersucht die Authentizität seiner eigenen ausführbaren Module. Sie können die Parameter für die Aufgabe **Integritätskontrolle für Anwendungen** nicht ändern. Sie können die Parameter des Zeitplans ändern oder den Start dieser Aufgabe nach dem Zeitplan deaktivieren.

Sie können *benutzerdefinierte Aufgaben* zur Virensuche erstellen. Beispielweise können Sie eine Aufgabe für die Untersuchung der gemeinsamen Ordner auf dem Server anlegen.

Anti-Virus kann gleichzeitig mehrere Aufgaben vom Typ Virensuche ausführen.

Details dazu, welche Kategorien von Aufgaben im Anti-Virus beim Erstellen und Ausführen vorgesehen sind, finden Sie in Pkt. 5.1 auf S. 52.

Details zu den Funktionen des Anti-Virus *Echtzeitschutz* und *Virensuche* finden Sie in Pkt. 1.1 auf S. 13.

Wie die Aufgaben in der Anti-Virus-Konsole der MMC verwaltet werden, finden Sie in Kapitel 5 auf S. 52.

9.2. Einstellung der Aufgaben zur Virensuche

Sie können die Systemaufgabe **Vollständige Untersuchung des Computers** sowie benutzerdefinierte Aufgabe zur Virensuche einstellen.

Wie eine benutzerdefinierte Aufgabe zur Virensuche angelegt wird, erfahren Sie in Pkt. 5.2 auf S. 54.

Um eine Aufgabe zur Virensuche einzustellen, machen Sie Folgendes:

1. In der Konsolenstruktur klappen Sie den Knoten **Virensuche** auf.
2. Klicken Sie auf die Aufgabe, die Sie einstellen wollen, um sie damit zu öffnen.
3. Passen Sie die Parameter der Aufgabe an: Erstellen Sie einen Untersuchungsbereich, bei Bedarf ändern Sie die Parameter für Sicherheit im gesamten Untersuchungsbereich oder für einzelne Knoten. Standardmäßig hat die Systemaufgabe **Vollständige Untersuchung des Computers** und ebenso jede neu angelegte benutzerdefinierte Aufgabe Parameter, die in der Tabelle 5 stehen.
4. Öffnen Sie das Kontextmenü mit einem Rechtsklick auf den Namen der Aufgabe und gehen Sie auf **Aufgabe speichern**, um die Änderungen in der Aufgabe zu speichern.

Tabelle 5. Standardmäßige Parameter für die Aufgabe **Vollständige Untersuchung des Computers**

Parameter	**Wert**	**Einstellungsmöglichkeit**
Untersuchungsbereich	gesamter Server Im Baum der File-Server-Ressourcen ist das Kontrollkästchen **Gemeinsame Ordner** nicht aktiviert – Anti-Virus untersucht gemeinsame Ordner nach ihrem tatsächlichen Pfad auf dem Laufwerk.	Sie können den Untersuchungsbereich einschränken (s. Pkt. 9.2.1 auf S. 124).
Parameter für Sicherheit	Einheitlich für den gesamten Untersuchungsbereich, entspricht der Sicherheitsstufe **Empfohlen**	Sie können für ausgewählte Knoten im Baum der File-Server-Ressourcen: • eine andere vordefinierte Sicherheitsstufe auswählen (s. Pkt. 9.2.2.1 auf S. 132) • manuell die Parameter für Sicherheit ändern (s. Pkt. 9.2.2 auf S. 131). Sie können die Parameter für Sicherheit des ausgewählten Knotens in eine Vorlage speichern, um sie später für andere Knoten zu übernehmen (s. Pkt. 9.2.2.3 auf S. 139).

Parameter	Wert	Einstellungsmöglichkeit
Vertrauenswürdige Zone	Wird verwendet. Ausgeschlossen werden Programme zur Remote-Administration **RemoteAdmin** und Dateien, die von der Firma Microsoft empfohlen werden, falls Sie bei der Installation von Anti-Virus die Optionen **Bedrohungen nach Maske not-a-virus:RemoteAdmin* zu Ausnahmen hinzufügen** und **Dateien zu Ausnahmen hinzufügen, die Microsoft empfiehlt** gewählt haben.	Einheitliche Liste der Ausnahmen, die Sie in ausgewählten Aufgaben zur Virensuche und in der Aufgabe **Echtzeitschutz für Dateien** verwenden können. Kapitel 8 auf S. 109 enthält Informationen über das Erstellen und die Verwendung der vertrauenswürdigen Zone.

9.2.1. Untersuchungsbereich in den Aufgaben zur Virensuche

In diesem Abschnitt stehen die folgenden Informationen:

- Anlegen eines Untersuchungsbereiches (s. Pkt. 9.2.1.1 auf S. 124)
- Vordefinierte Bereiche (s. Pkt. 9.2.1.2 auf S. 125)
- Erstellen von Untersuchungsbereichen (s. Pkt. 9.2.1.3 auf S. 127)
- Übernehmen eines Netzwerkpfades in einen Untersuchungsbereich (s. Pkt. 9.2.1.4 auf S. 128)
- Erstellen eines virtuellen Untersuchungsbereiches – Übernahme eines dynamischen Datenträgers, Ordners und Datei in den Untersuchungsbereich (s. Pkt. 9.2.1.5 auf S. 129)

9.2.1.1. Untersuchungsbereich in den Aufgaben zur Virensuche anlegen

Standardmäßig wird in der Systemaufgabe **Vollständige Untersuchung des Computers** sowie in neu angelegten Aufgaben zur Virensuche der gesamte

Server in den Untersuchungsbereich übernommen. Wenn aus Sicherheitsgründen nicht alles untersucht werden muss, können Sie den Untersuchungsbereich auf nur einige Serverbereiche einschränken.

In der Anti-Virus-Konsole ist der Untersuchungsbereich ein Baum der File-Server-Ressourcen, die Anti-Virus untersuchen kann.

Die Knoten im Baum der File-Server-Ressourcen werden auf folgende Weise dargestellt:

- Der Knoten ist im Untersuchungsbereich.
- Der Knoten ist nicht im Untersuchungsbereich.
- Mindestens ein in diesem Knoten eingebetteter Knoten ist nicht im Untersuchungsbereich oder die Sicherheitsparameter des eingebetteten Knotens unterscheiden sich von den Sicherheitsparametern dieses Knotens.

Die Namen der virtuellen Knoten in einem Untersuchungsbereich werden mit Schrift in blauer Farbe angezeigt.

9.2.1.2. Vordefinierte Untersuchungsbereiche

Um den Baum der File-Server-Ressourcen anzuzeigen, machen Sie Folgendes:

1. In der Konsolenstruktur klappen Sie den Knoten **Virensuche** auf.
2. Markieren Sie die Aufgabe zur Virensuche, deren Untersuchungsbereich Sie anzeigen wollen, um sie damit zu öffnen (s. Abbildung 41).



Abbildung 41. Beispiel für Baum der File-Server-Ressourcen in der Anti-Virus-Konsole

Im Ergebnisfenster wird der Baum der Dateiserver-Ressourcen dargestellt, aus dessen Objekten Sie einen Untersuchungsbereich erstellen können.

Der Baum der Server-Dateiressourcen enthält die folgenden Bereiche:

- **Arbeitsplatz** Anti-Virus untersucht den gesamten Server.
- **Festplatten** Anti-Virus untersucht Objekte auf den Festplatten des Servers. Sie können in den Untersuchungsbereich alle Festplatten sowie einzelne Datenträger, Ordner oder Dateien aufnehmen oder ausschließen.
- **Wechseldatenträger**. Anti-Virus untersucht Objekte auf Wechseldatenträgern, zum Beispiel auf CD-ROMs oder USB-Sticks. Sie können in den Untersuchungsbereich alle Wechseldatenträger sowie einzelne Datenträger, Ordner oder Dateien aufnehmen oder ausschließen.
- **Systemspeicher**. Anti-Virus untersucht den System- und Prozessspeicher.
- **Autostart-Objekte**: Anti-Virus untersucht Objekte, auf die Registry-Schlüssel und Konfigurationsdateien verweisen, zum Beispiel die WIN.INI oder SYSTEM.INI sowie Programm-Module von Anwendungen, die automatisch beim Computerstart geladen werden.
- **Gemeinsame Ordner**. Anti-Virus untersucht alle gemeinsamen Ordner auf dem geschützten Server.
- **Netzwerkumgebung**. Sie können in den Untersuchungsbereich Netzwerkordnern oder Dateien aufnehmen, indem Sie die Netzwerkpfade im UNC-Format (Universal Naming Convention) eingeben. Das Benutzerkonto, das Sie für den Aufgabenstart verwenden, muss die Berechtigungen für diese hinzugefügten Netzwerkordner haben. In der Grundeinstellung wird jede Aufgabe zur Virensuche mit dem Benutzerkonto **Lokales System** (**SYSTEM**) ausgeführt. Details s. Pkt. 9.2.1.4 auf S. 128.
- **Virtuelle Laufwerke**. Sie können in den Untersuchungsbereich dynamische Datenträger, Ordner und Dateien sowie Datenträger aufnehmen, die auf dem Server überwacht werden, beispielsweise allgemeine Datenträger eines Clusters (Anlegen eines *virtuellen Schutzbereiches*). Details s. Pkt. 9.2.1.5 auf S. 129.

Anmerkung

Pseudo-Datenträger, die mit SUBST erzeugt worden sind, werden im Baum der File-Server-Ressourcen in der Anti-Virus-Konsole nicht dargestellt. Um Objekte auf einem Pseudo-Datenträger zu untersuchen, übernehmen Sie den Ordner in den Untersuchungsbereich, mit dem der Pseudo-Datenträger verknüpft ist.

Die angeschlossenen Netzwerk-Datenträger werden im Baum der File-Server-Ressourcen nicht dargestellt. Um Objekte auf dem Netzwerk-Datenträger in den Untersuchungsbereich zu übernehmen, geben Sie den Pfad zum Ordner, der diesem Netzwerk-Datenträger entspricht, im UNC-Format (Universal Naming Convention) ein.

9.2.1.3. Erstellen eines Schutzbereiches

Wenn Sie Anti-Virus auf dem geschützten Server im Remote-Betrieb über die MMC-Konsole verwalten, die auf dem Desktop des Administrators installiert ist, müssen Sie zur Gruppe der lokalen Administratoren auf dem geschützten Server gehören, um die dort befindlichen Ordner zu sehen.

Um einen Untersuchungsbereich anzulegen, machen Sie Folgendes:

1. In der Konsolenstruktur klappen Sie den Knoten **Virensuche** auf.
2. Markieren Sie die Aufgabe zur Virensuche, deren Untersuchungsbereich Sie erstellen wollen.

   Im Ergebnisfenster wird der Baum der File-Server-Ressourcen dargestellt. In der Grundeinstellung sind alle Bereiche des geschützten Servers im Untersuchungsbereich enthalten.
3. Führen Sie die folgenden Aktionen aus:
   - Um die Knoten auszuwählen, die Sie zum Untersuchungsbereich hinzufügen wollen, entfernen Sie das Häkchen vor **Arbeitsplatz**, und führen Sie die folgenden Aktionen aus:
     - Wenn Sie alle Datenträger eines Typs in den Untersuchungsbereich nehmen wollen, setzen Sie das Häkchen neben dem Namen des gewünschten Datenträgertyps.
     - wenn Sie einen einzelnen Datenträger in den Untersuchungsbereich nehmen wollen, klappen Sie den Knoten auf, der die Liste mit den Datenträgern dieses Typs enthält, und setzen Sie das Häkchen neben dem Namen des gewünschten Datenträgers. Um zum Beispiel den Wechseldatenträger **F:** auszuwählen, klappen Sie den Knoten **Wechseldatenträger** auf und setzen Sie das Häkchen für den Datenträger **F:**.

        - Wenn Sie einen einzelnen Ordner auf einem Datenträger in den Untersuchungsbereich nehmen wollen, klappen Sie den Baum der Server-Dateiressourcen auf, um den gewünschten Ordner anzuzeigen, und setzen Sie das Häkchen neben dessen Namen. Auf die gleiche Weise können Sie auch Dateien in den Untersuchungsbereich aufnehmen.

    - Zum Ausschließen eines einzelnen Knoten aus dem Untersuchungsbereich klappen Sie den Baum des Untersuchungsbereiches auf, um den gewünschten Knoten dazustellen, und Sie entfernen das Häkchen neben seinem Namen.

4. Öffnen Sie das Kontextmenü mit einem Rechtsklick auf den Namen der Aufgabe und gehen Sie auf **Aufgabe speichern**, um die Änderungen an der Aufgabe zu speichern.

So aktivieren Sie einen Untersuchungsbereich:

- Netzwerk-Datenträger, -Ordner oder -Datei (s. Pkt. 9.2.1.4 auf S. 128)
- dynamischer Datenträger, Ordner oder Datei (s. Pkt. 9.2.1.5 auf S. 129)

9.2.1.4. Netzwerk-Datenträger, -Ordner oder - Dateien in Schutzbereich übernehmen

Sie können in den Untersuchungsbereich Netzwerk-Datenträger, -Ordner oder - Dateien aufnehmen, indem Sie die Netzwerkpfade im UNC-Format (Universal Naming Convention) eingeben.

Um ein Netzwerkobjekt dem Untersuchungsbereich hinzuzufügen, machen Sie Folgendes:

1. In der Konsolenstruktur klappen Sie den Knoten **Virensuche** auf.
2. Markieren Sie die Aufgabe zur Virensuche, deren Untersuchungsbereich Sie einen Netzwerkpfad hinzufügen wollen.
3. Öffnen Sie das Kontextmenü für den Knoten **Netzwerkumgebung** und wählen Sie den Befehl **Netzwerkordner hinzufügen** oder **Netzwerkdatei hinzufügen**.
4. Geben Sie den Pfad zum Netzwerkordner oder zur Netzwerkdatei im UNC-Format (Universal Naming Convention) ein und klicken Sie auf **<ENTER>**.
5. Setzen Sie das Häkchen neben dem hinzugefügten Netzwerkobjekt, um es für den Untersuchungsbereich zu übernehmen.

6. Bei Bedarf ändern Sie die Parameter für Sicherheit des hinzugefügten Netzwerkobjektes (s. Pkt. 9.2.2 auf S. 131).
7. Öffnen Sie das Kontextmenü mit einem Rechtsklick auf den Namen der Aufgabe und gehen Sie auf **Aufgabe speichern**, um die Änderungen in der Aufgabe zu speichern.

9.2.1.5. Virtuelle Untersuchungsbereiche erstellen: Dynamische Datenträger, Ordner oder Dateien in Untersuchungsbereich übernehmen

Sie können in den Untersuchungsbereich dynamische Datenträger, Ordner und Dateien sowie Datenträger aufnehmen, die auf dem Server überwacht werden, beispielsweise allgemeine Datenträger eines Clusters (Anlegen eines *virtuellen Schutzbereiches*). Details zu einem virtuellen Untersuchungsbereich finden Sie in Pkt. 6.2.1.4 auf S. 76.

Sie können einem virtuellen Untersuchungsbereich dynamische Datenträger, Ordner oder Dateien hinzufügen.

Um einen virtuellen Datenträger zu einem Untersuchungsbereich hinzuzufügen, machen Sie Folgendes:

1. In der Konsolenstruktur klappen Sie den Knoten **Virensuche** auf.
2. Markieren Sie die Aufgabe zur Virensuche, in der Sie einen virtuellen Untersuchungsbereich erstellen wollen, um die Aufgabe zu öffnen.
3. Im Ergebnisfenster öffnen Sie im Baum der File-Server-Ressourcen das Kontextmenü für den Knoten **Virtuelle Datenträger** und in der Liste mit den verfügbaren Namen wählen Sie einen Namen für den anzulegenden virtuellen Datenträger (s. Abbildung 42).

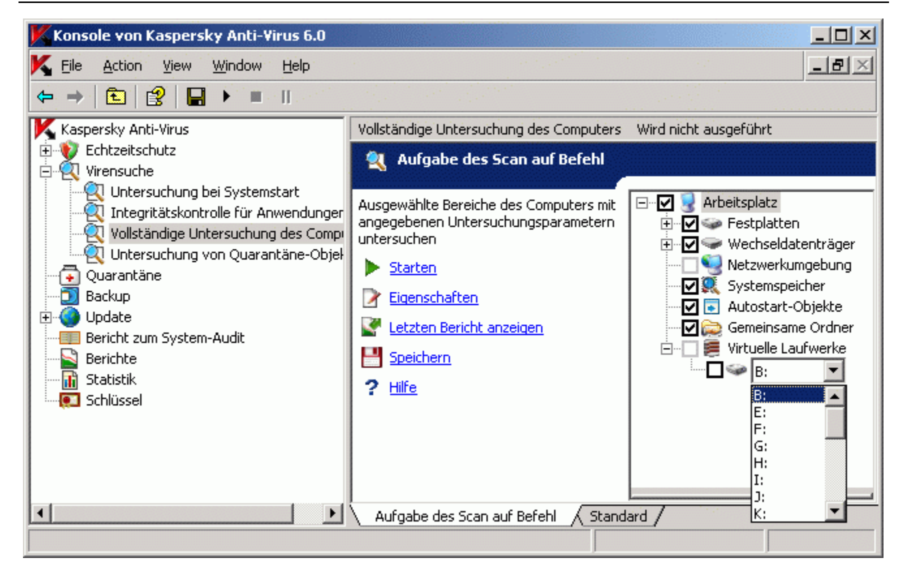


Abbildung 42. Namen für anzulegenden virtuellen Datenträger auswählen

4. Setzen Sie das Häkchen neben dem hinzugefügten Datenträger, um den Datenträger in den Untersuchungsbereich zu übernehmen.
5. Öffnen Sie das Kontextmenü mit einem Rechtsklick auf den Namen der Aufgabe und gehen Sie auf **Aufgabe speichern**, um die Änderungen in der Aufgabe zu speichern.

Um einen virtuellen Ordner oder eine virtuelle Datei zum Untersuchungsbereich hinzuzufügen, machen Sie Folgendes:

1. In der Konsolenstruktur klappen Sie den Knoten **Virensuche** auf.
2. Markieren Sie die Aufgabe zur Virensuche, in der Sie einen virtuellen Untersuchungsbereich erstellen wollen, um die Aufgabe zu öffnen.
3. Im Ergebnisfenster öffnen Sie im Baum der File-Server-Ressourcen mit der rechten Maustaste das Kontextmenü des Knotens, in den Sie einen Ordner oder eine Datei einfügen wollen, und gehen auf **Virtuellen Ordner hinzufügen** oder **Virtuelle Datei hinzufügen**.

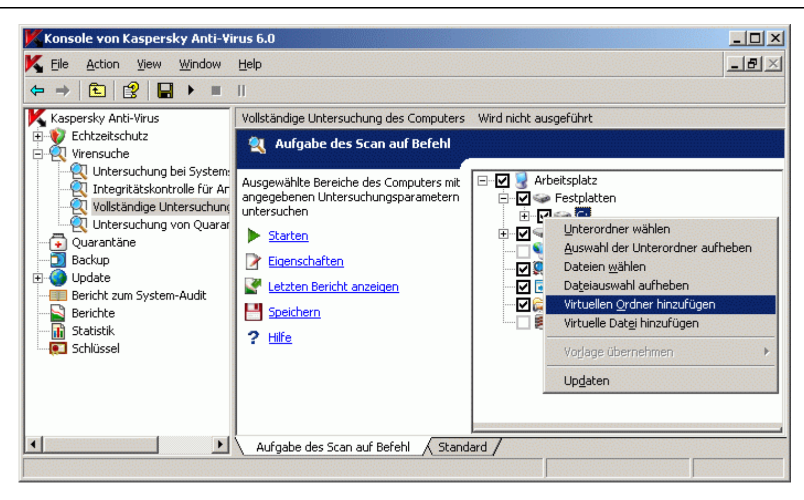


Abbildung 43. Virtuellen Ordner hinzufügen

4. In das Eingabefeld tragen Sie den Namen für den Ordner (die Datei) ein. Sie können eine Maske für den Namen des Ordners (der Datei) eingeben. Für Masken dürfen die Sonderzeichen * und ? verwendet werden.

5. In der Zeile mit dem Namen des erstellten Ordners (der erstellten Datei) setzen Sie das Häkchen, um den Ordner (die Datei) in den Untersuchungsbereich zu übernehmen.

6. Öffnen Sie das Kontextmenü mit einem Rechtsklick auf den Namen der Aufgabe und gehen Sie auf **Aufgabe speichern**, um die Änderungen in der Aufgabe zu speichern.

9.2.2. Parameter für Sicherheit für ausgewählten Knoten einstellen

In einer ausgewählten Aufgabe zur Virensuche können Sie die Parameter für Sicherheit für den gesamten Untersuchungsbereich einheitlich oder für verschiedene Knoten im Baum der File-Server-Ressourcen unterschiedlich einstellen. Die Parameter für Sicherheit, die Sie für einen ausgewählten Knoten einstellen können, werden automatisch für alle Knoten übernommen, die darin eingebettet sind. Wenn Sie jedoch die Parameter für Sicherheit eines eingebetteten Knoten separat einstellen, dann werden die Parameter für Sicherheit des übergeordneten Knoten für ihn nicht übernommen.

Sie können die Parameter eines ausgewählten Untersuchungsbereiches auf eine der folgenden Weisen einstellen:

- Auswählen unter einer der drei vordefinierten Sicherheitsstufen (Maximales Tempo, Empfohlen oder Maximale Sicherheit) (s. Pkt. 9.2.2.1 auf S. 132)
- Manuelles Ändern der Parameter für Sicherheit ausgewählter Knoten im Baum der File-Server-Ressourcen (s. Pkt. 9.2.2.2 auf S. 135).

Sie können den Parametersatz eines Knotens in eine Vorlage speichern, um später diese Vorlage für andere Knoten zu übernehmen (s. Pkt. 9.2.2.3 auf S. 139).

9.2.2.1. Vordefinierte Sicherheitsstufe in den Aufgaben zur Virensuche auswählen

Für einen ausgewählten Knoten im Baum der File-Server-Ressourcen können Sie eine der vordefinierten Sicherheitsstufen übernehmen: a) maximales Tempo, b) empfohlen und c) maximale Sicherheit. Jede vordefinierte Sicherheitsstufe hat eigene Parameterwerte für die Sicherheit. Diese Parameter stehen in der Tabelle 6.

Maximales Tempo

Sie können die Sicherheitsstufe **Maximales Tempo** aktivieren, wenn in Ihrem Netzwerk neben dem Anti-Virus auf den Servern und Workstations zusätzliche Maßnahmen für die Computersicherheit getroffen worden sind, beispielsweise Firewalls installiert wurden und Sicherheitsrichtlinien für die Netzwerkbenutzer in Kraft sind.

Empfohlen

Die Sicherheitsstufe **Empfohlen** ist standardmäßig aktiviert. Diese Sicherheitsstufe reicht nach den Einschätzungen von Kaspersky Lab für die Untersuchung von File-Servern in den meisten Netzwerken aus. Sie sorgt für eine optimale Qualität der Untersuchung und deren Tempo.

Maximaler Schutz

Verwenden Sie die Sicherheitsstufe **Maximaler Schutz**, wenn Sie für die Computersicherheit in einem Netzwerk keine anderen Maßnahmen angesetzt haben.

Wie Sie die Parameter für Sicherheit bei einem ausgewählten Knoten im Baum der Server-Dateiressourcen von Hand einstellen, finden Sie in Pkt. 9.2.2 auf S. 131.

Tabelle 6. Vordefinierte Sicherheitsstufen und entsprechende Parameterwerte für Sicherheit

Parameter	**Vordefinierte Sicherheitsstufe**		
	Maximales Tempo	**Empfohlen**	**Maximale Sicherheit**
Zu untersuchende Objekte (s. Pkt. B.3.2 auf S. 397)	Nach Format	Alle Objekte	Alle Objekte
Nur neue und veränderte Objekte untersuchen (s. Pkt. B.3.3 auf S. 399)	Aktiviert	Deaktiviert	Deaktiviert
Aktion für infizierte Objekte (s. Pkt. B.3.5 auf S. 401)	Desinfizieren, löschen, wenn Desinfizieren nicht möglich ist	Desinfizieren, löschen, wenn Desinfizieren nicht möglich ist	Desinfizieren, löschen, wenn Desinfizieren nicht möglich ist
Aktion für verdächtige Objekte (s. Pkt. B.3.6 auf S. 403)	In Quarantäne verschieben	In Quarantäne verschieben	In Quarantäne verschieben
Objekte ausschließen (s. Pkt. B.3.8 auf S. 407)	Nein	Nein	Nein
Bedrohungen ausschließen (s. Pkt. B.3.9 auf S. 408)	Nein	Nein	Nein
Maximale Dauer der Objekt-Untersuchung (s. Pkt. B.3.10 auf S. 409)	60 Sek.	Nein	Nein
Maximale Größe des zu untersuchenden Compound-Objektes (s. Pkt. B.3.11 auf S. 410)	8 MB	Nein	Nein
Zusätzliche Ströme des Dateisystems (NTFS) untersuchen (s. Pkt. B.3.2 auf S. 397)	Ja	Ja	Ja

Parameter	Vordefinierte Sicherheitsstufe		
	Maximales Tempo	**Empfohlen**	**Maximale Sicherheit**
Bootsektoren untersuchen (s. Pkt. B.3.2 auf S. 397)	Ja	Ja	Ja
Compound-Objekte untersuchen (s. Pkt. B.3.4 auf S. 400)	• SFX-Archive* • Gepackte Objekte* • Eingebettete OLE-Objekte* *Nur neue und veränderte	• Archive* • SFX-Archive* • Gepackte Objekte* • Eingebettete OLE-Objekte* *Alle Objekte	• Archive* • SFX-Archive* • Mail-Datenbanken* • Dateien in Mail-Formaten* • Gepackte Objekte* • Eingebettete OLE-Objekte* *Alle Objekte

Anmerkung

Beachten Sie, dass die Parameter für Sicherheit **Übernahme von iChecker™** und **Übernahme von iSwift™** nicht zum Parametersatz der vordefinierten Sicherheitsstufen gehören. Als Standard sind diese Parameter aktiviert. Wenn Sie den Status der Parameter **Übernahme von iChecker™** und **Übernahme von iSwift™** ändern, bleibt die vordefinierte Sicherheitsstufe davon unberührt.

Um eine vordefinierte Sicherheitsstufe auszuwählen, machen Sie Folgendes:

1. In der Konsolenstruktur markieren Sie den Knoten **Virensuche**.
2. Markieren Sie die Aufgabe zur Virensuche, in dem Sie die Parameter für Sicherheit einstellen wollen.
3. Im Ergebnisfenster markieren Sie den Knoten des Untersuchungsbereiches, für den Sie eine vordefinierte Sicherheitsstufe auswählen wollen.
4. Vergewissern Sie sich, dass dieser Knoten zum Untersuchungsbereich gehört (s. Pkt. 9.2.1.1 auf S. 124).
5. Im Dialogfenster **Sicherheitsstufe** (s. Abbildung 44) wählen Sie die Sicherheitsstufe, die Sie übernehmen wollen.

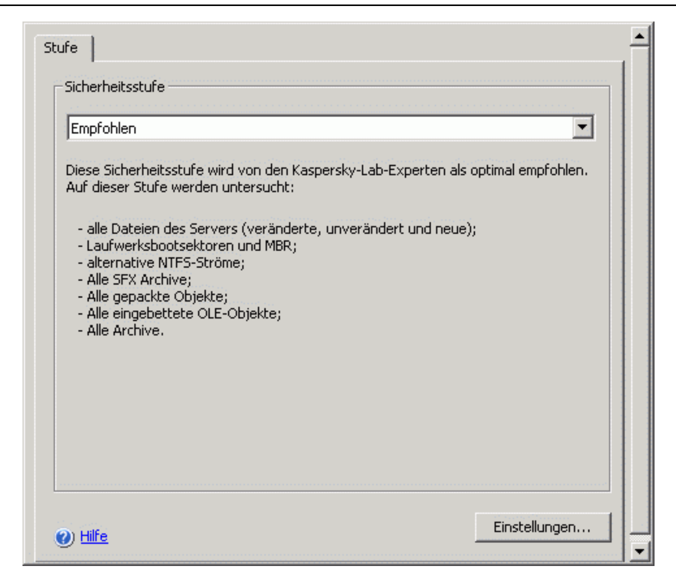


Abbildung 44. Dialogfenster **Sicherheitsstufe**

Im Dialogfenster wird die Liste der Parameterwerte für Sicherheit dargestellt, die der von Ihnen ausgewählten Sicherheitsstufe entsprechen.

6. Öffnen Sie das Kontextmenü mit einem Rechtsklick auf den Namen der Aufgabe und gehen Sie auf **Aufgabe speichern**, um die Änderungen in der Aufgabe zu speichern.

9.2.2.2. Parameter für Sicherheit von Hand einstellen

Um die Parameter für Sicherheit manuell einzustellen, machen Sie Folgendes:

1. In der Konsolenstruktur markieren Sie den Knoten **Virensuche**.
2. Markieren Sie die Aufgabe zur Virensuche, in dem Sie die Parameter für Sicherheit einstellen wollen.
3. Im Ergebnisfenster markieren Sie den Knoten des Untersuchungsbereiches, dessen Parameter für Sicherheit Sie einstellen wollen. Vergewissern Sie sich, dass dieser Knoten zum Untersuchungsbereich gehört (Details zur Erstellung eines Untersuchungsbereiches finden Sie in Pkt. 9.2.1.3 auf S. 127).

   Im unteren Teil des Ergebnisfensters wird das Dialogfenster **Sicherheitsstufe** angezeigt (s. Abbildung 45).

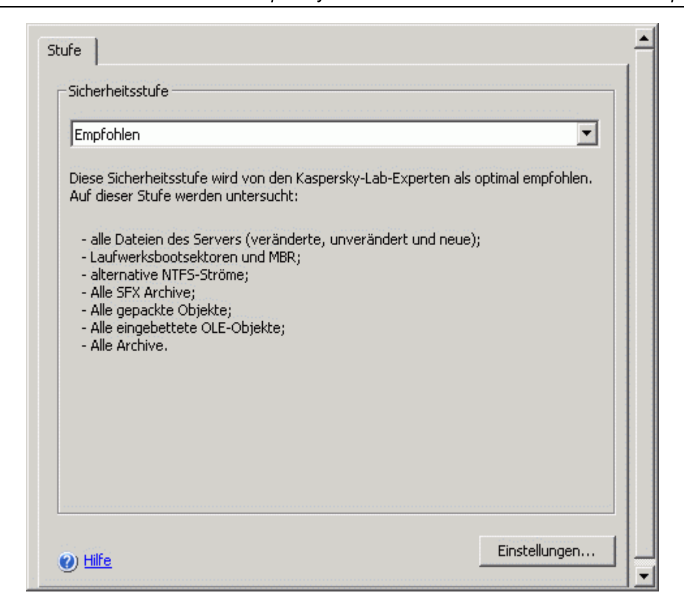


Abbildung 45. Dialogfenster **Sicherheitsstufe**

Klicken Sie auf die Schaltfläche **Einstellungen**, um das Dialogfenster **Parameter für Sicherheit** zu öffnen.

> **Anmerkung**
>
> Sie können das Dialogfenster **Parameter für Sicherheit** für einen markierten Knoten im Baum der Dateiressourcen öffnen, indem Sie das Kontextmenü mit einem Rechtsklick auf diesen Knoten öffnen und auf **Eigenschaften** gehen.

4. Im Dialogfenster **Parameter für Sicherheit** konfigurieren Sie die gewünschten Parameter für Sicherheit je nach Ihren Wünschen.

   - Auf der Registerkarte **Allgemein** (s. Abbildung 46) führen Sie die folgenden Aktionen aus:

     - Unter der Überschrift **Untersuchung von Objekten** bestimmen Sie, ob Anti-Virus alle Objekte des Untersuchungsbereiches oder nur die Objekte mit bestimmten Formaten oder bestimmten Erweiterungen untersuchen soll, ob Anti-Virus die Boot-Sektoren und MBR, alternative NTFS-Datenströme untersuchen soll (s. Pkt. B.3.2 auf S. 397).

- Legen Sie im Abschnitt **Optimierung** fest, ob Anti-Virus im ausgewählten Bereich alle Objekte untersuchen soll oder nur neue und veränderte Objekte (s. Pkt. B.3.3 auf S. 399).
- Unter der Überschrift **Untersuchung von zusammengesetzten Objekten** geben Sie an, welche Compound-Objekte Anti-Virus untersuchen soll (s. Pkt. B.3.4 auf S. 400).

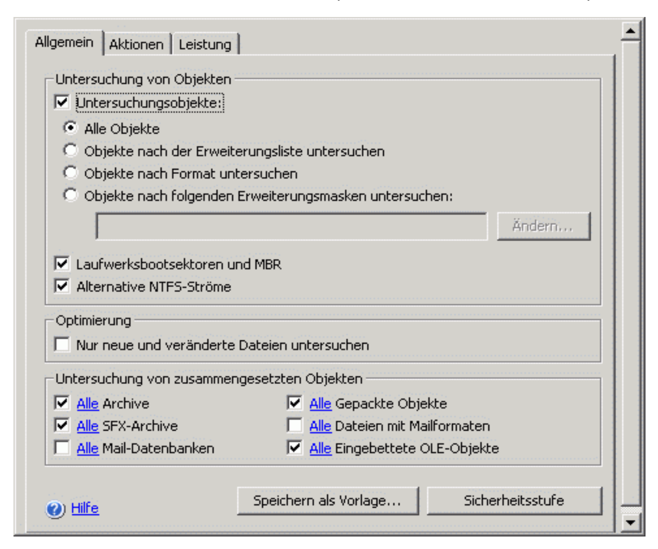


Abbildung 46. Dialogfenster **Parameter für Sicherheit** der Aufgabe **Virensuche**, Registerkarte **Allgemein**

- Auf der Registerkarte **Aktionen** (s. Abbildung 47) führen Sie die folgenden Aktionen aus:
  - Wählen Sie eine Aktion für infizierte Objekte aus (s. Pkt. B.3.5 auf S. 401).
  - Wählen Sie eine Aktion für verdächtige Objekte aus (s. Pkt. B.3.6 auf S. 403).
  - Bei Bedarf konfigurieren Sie die Aktionen für Objekte je nach Typ der im Objekt gefundenen Bedrohung (s. Pkt. B.3.7 auf S. 405).

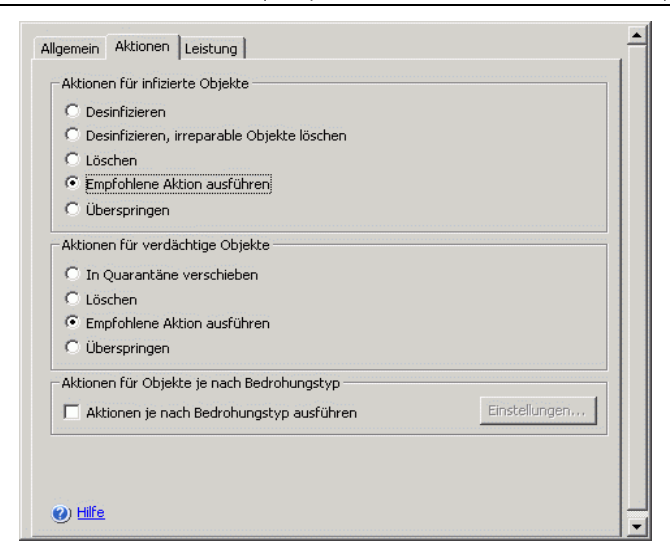


Abbildung 47. Dialogfenster **Parameter für Sicherheit** der Aufgabe **Virensuche**, Registerkarte **Aktionen**

- Auf der Registerkarte **Leistung** (s. Abbildung 48) führen Sie bei Bedarf die folgenden Aktionen aus:
  - Schließen Sie Dateien nach Name oder Maske aus (s. Pkt. B.3.8 auf S. 407).
  - Schließen Sie Bedrohungen nach Name oder Namensmaske aus (s. Pkt. B.3.9 auf S. 408).
  - Geben Sie die maximale Dauer der Objekt-Untersuchung an (s. Pkt. B.3.10 auf S. 409).
  - Geben Sie die maximale Größe des zu untersuchenden Compound-Objektes an (s. Pkt. B.3.11 auf S. 410).
  - Aktivieren oder deaktivieren Sie die Übernahme von iChecker™ (s. Pkt. B.3.12 auf S. 410).
  - Aktivieren oder deaktivieren Sie die Übernahme von iSwift™ (s. Pkt. B.3.13 auf S. 411).

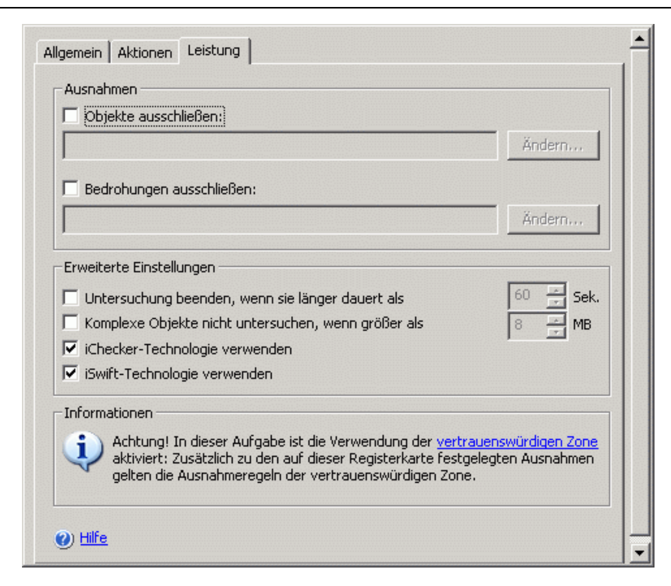


Abbildung 48. Dialogfenster **Parameter** der Aufgabe **Virensuche**, Registerkarte **Leistung**

5. Nachdem Sie die gewünschten Parameter für Sicherheit eingestellt haben, öffnen Sie das Kontextmenü mit einem Rechtsklick auf den Namen der Aufgabe und gehen Sie auf **Aufgabe speichern**, um die Änderungen an der Aufgabe zu speichern.

9.2.2.3. Vorlagen in den Aufgaben zur Virensuche

In diesem Abschnitt stehen die folgenden Informationen:

- Speichern eines Parametersatzes für Sicherheit in Vorlage (s. Pkt. 9.2.2.3.1 auf S. 140)
- Parameter für Sicherheit in Vorlage anzeigen (s. Pkt. 9.2.2.3.2 auf S. 141)
- Übernehmen einer Vorlage (s. Pkt. 9.2.2.3.3 auf S. 142)
- Löschen einer Vorlage (s. Pkt. 9.2.2.3.4 auf S. 143)

9.2.2.3.1. Speichern eines Parametersatzes für Sicherheit in Vorlage

Nachdem Sie die Parameter eines beliebigen Knotens im Baum der File-Server-Ressourcen eingestellt haben, können Sie in der Aufgabe zur Virensuche diesen Parametersatz in einer Vorlage speichern, um sie später für einen anderen Knoten zu übernehmen.

Um einen Parametersatz in einer Vorlage zu speichern, machen Sie Folgendes:

1. In der Konsolenstruktur markieren Sie den Knoten **Virensuche**.
2. Markieren Sie die Aufgabe zur Virensuche, dessen Parameter für Sicherheit Sie in einer Vorlage speichern wollen.
3. Im Baum der File-Server-Ressourcen markieren Sie einen Knoten, dessen Parameter für Schutz Sie speichern wollen.
4. Im Dialogfenster **Parameter für Sicherheit** klicken Sie auf der Registerkarte **Allgemein** auf die Schaltfläche **Speichern als Vorlage**.
5. Im Dialogfenster **Eigenschaften der Vorlage** (s. Abbildung 49) machen Sie Folgendes:
   - Geben Sie im Feld **Vorlagenname** den Namen der Vorlage ein.
   - Im Feld **Beschreibung** tragen Sie beliebige Zusatzinformationen zur Vorlage ein.



Abbildung 49. Dialogfenster **Eigenschaften der Vorlage**

6. Klicken Sie auf die Schaltfläche **OK**. Die Vorlage wird mit dem Parametersatz gespeichert.

9.2.2.3.2. Parameter für Sicherheit in Vorlage anzeigen

Um die Werte der Parameter für Sicherheit in einer vorhandenen Vorlage anzuzeigen, machen Sie Folgendes:

1. In der Konsolenstruktur öffnen Sie das Kontextmenü für den Knoten **Virensuche** und gehen Sie auf **Vorlagen** (s. Abbildung 50).

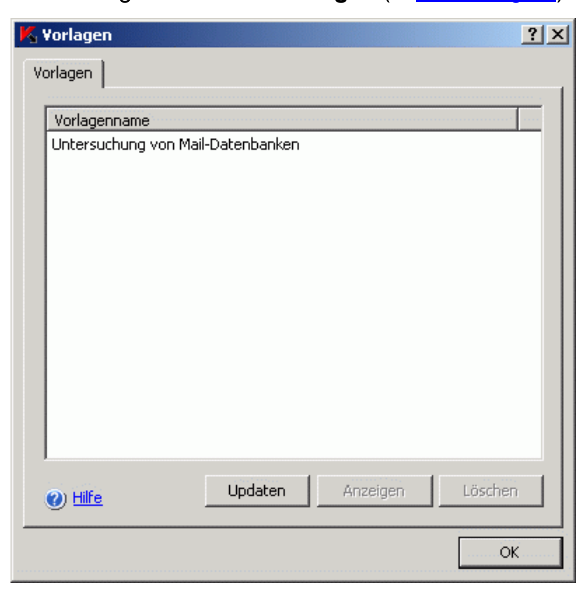


Abbildung 50. Dialogfenster **Vorlagen**

Im Dialogfenster **Vorlagen** steht eine Liste von Vorlagen, die Sie in die Aufgaben zur Virensuche übernehmen können.

2. Um Daten über die Vorlage und die Werte der Parameter für Sicherheit anzuzeigen, markieren Sie die gewünschte Vorlage in der Liste und klicken Sie auf die Schaltfläche **Anzeigen** (s. Abbildung 51).

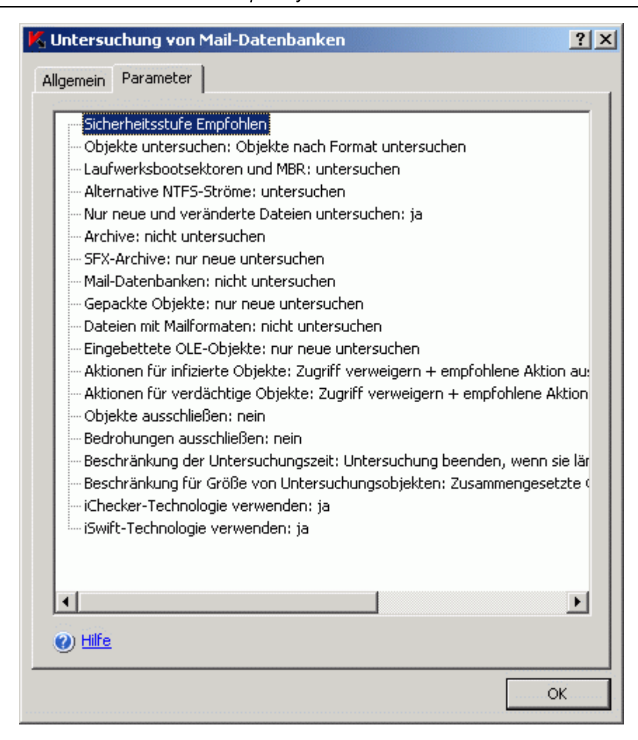


Abbildung 51. Dialogfenster **<Vorlagenname>**, Registerkarte **Parameter**

Auf der Registerkarte **Allgemein** werden der Name der Vorlage und zusätzliche Informationen über die Vorlage dargestellt. Auf der Registerkarte **Parameter** steht die Liste mit den Werten der Parameter für Sicherheit, die in der Vorlage gespeichert sind.

9.2.2.3.3. Vorlage übernehmen

Um eine Vorlage mit einem Satz von Parametern für Sicherheit zu übernehmen, machen Sie Folgendes:

1. Speichern Sie vorsichtshalber die Werte der Parameter für Sicherheit in einer Vorlage (s. Anweisungen in Pkt. 9.2.2.3.1 auf S. 140).
2. In der Konsolenstruktur markieren Sie den Knoten **Virensuche**.
3. Markieren Sie die Aufgabe zur Virensuche, in der Sie die Parameter für Sicherheit übernehmen wollen.

4. Im Baum der File-Server-Ressourcen öffnen Sie mit einem Rechtsklick auf den Knoten, für den Sie eine Vorlage übernehmen wollen, und gehen auf **Vorlage übernehmen** → **<Vorlagenname>**.

5. Im Vorlagenverzeichnis suchen Sie die Vorlage, die Sie übernehmen wollen.

6. Im Dialogfenster **Parameter für Sicherheit** klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern.

Hinweis

Wenn Sie für einen übergeordneten Knoten eine Vorlage übernehmen, werden die Sicherheitsparameter der Vorlage auch für alle untergeordneten Knoten übernommen, unter Ausnahme jener, für welche die Sicherheitsparameter separat angepasst wurden.

Um die Sicherheitsparameter der Vorlage für alle untergeordneten Knoten zu übernehmen, deaktivieren Sie vor dem Übernehmen der Vorlage in der Struktur der Dateiressourcen des Servers das Kontrollkästchen des übergeordneten Knotens, und aktivieren Sie es anschließend wieder. Übernehmen Sie die Vorlage für den übergeordneten Knoten. Alle untergeordneten Knoten erhalten nun die gleichen Sicherheitsparameter wie der übergeordnete Knoten.

9.2.2.3.4. Vorlage löschen

Um eine Vorlage zu löschen, machen Sie Folgendes:

1. In der Konsolenstruktur öffnen Sie das Kontextmenü für den Knoten **Virensuche** und gehen Sie auf **Vorlagen** (s. Abbildung 50).

2. Im Dialogfenster **Vorlagen** markieren Sie in der Vorlagenliste die Vorlage, die Sie löschen wollen, und klicken Sie auf die Schaltfläche **Löschen**.

3. Im Dialogfenster zur Bestätigung klicken Sie auf die Schaltfläche **Ja**. Die ausgewählte Vorlage wird gelöscht.

9.3. Aufgaben zur Virensuche im Hintergrund

In der Grundeinstellung haben Prozesse, die Aufgaben des Anti-Virus ausführen, die Basispriorität **Mittel** (**Normal**).

Sie können einem Prozess, in dem eine Aufgabe zur Virensuche ausgeführt wird, die Basispriorität **Niedrig** (**Low**) zuweisen. Das Senken der Priorität eines

Prozesses verlängert die Aufgabenausführung und beeinflusst positiv das Tempo der Prozessausführung von anderen aktiven Anwendungen.

In einem Prozess mit niedriger Priorität können mehrere Aufgaben im Hintergrund erledigt werden. Sie können die maximale Anzahl der Prozesse von Aufgaben zur Virensuche im Hintergrund angeben (s. Pkt. B.1.3 auf S. 378).

Sie können die Aufgabenpriorität beim Erstellen oder später im Dialogfenster **Eigenschaften der Aufgabe** angeben.

Um die Priorität einer Aufgabe zur Virensuche zu ändern, machen Sie Folgendes:

1. In der Konsolenstruktur klappen Sie den Knoten **Virensuche** auf.
2. Öffnen Sie das Kontextmenü mit einem Rechtsklick auf die Aufgabe, deren Priorität Sie ändern wollen, und gehen Sie auf **Eigenschaften**.

   Es öffnet sich das Dialogfenster **Eigenschaften: <Aufgabe>** (s. Abbildung 52).

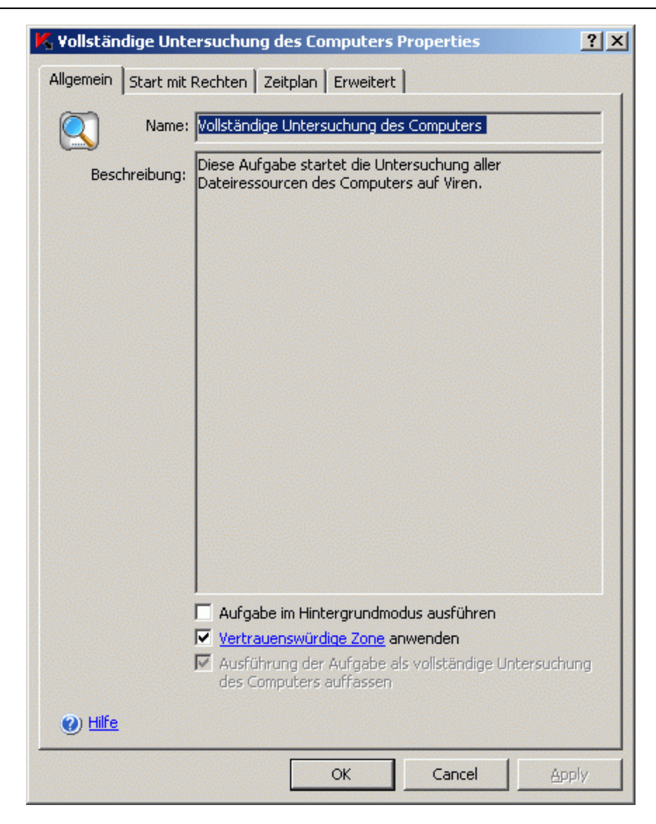


Abbildung 52. Dialogfenster **Eigenschaften: <Aufgabe>**

3. Auf der Registerkarte **Allgemein** führen Sie eine der folgenden Aktionen aus:

   - Um den Hintergrund-Modus für die Aufgabenausführung zu aktivieren, setzen Sie das Häkchen in **Aufgabe im Hintergrundmodus ausführen**.

   - Um den Hintergrund-Modus für die Aufgabenausführung zu deaktivieren, entfernen Sie das Häkchen in **Aufgabe im Hintergrundmodus ausführen**.

Anmerkung

Wenn Sie den Hintergrund-Modus für die Aufgabenausführung aktivieren oder deaktivieren, wird die Priorität der Aufgabe nicht unmittelbar geändert, sondern erst beim nächsten Start.

9.4. Statistik von Aufgaben zur Virensuche

Solange die Aufgabe zur Virensuche ausgeführt wird, können Sie Detailinformationen zur Anzahl der Objekte, die Anti-Virus seit dem Aufgabenstart bis jetzt verarbeitet hat, im Dialogfenster **Statistik** anzeigen lassen.

Wenn Sie die Aufgabe anhalten und fortsetzen, wird die Statistik gespeichert. Nach dem Abschluss (Beenden) der Aufgabe steht die Aufgabenstatistik im Knoten **Berichte** (s. Pkt. 13.2.4 auf S. 210) zur Verfügung.

Um die Statistik für eine Aufgabe zur Virensuche anzuzeigen, machen Sie Folgendes:

1. In der Konsolenstruktur klappen Sie den Knoten **Virensuche** auf.
2. Öffnen Sie das Kontextmenü mit einem Rechtsklick auf die Aufgabe zur Virensuche, deren Statistik Sie anzeigen wollen, und gehen Sie auf **Statistik anzeigen** (s. Abbildung 53).

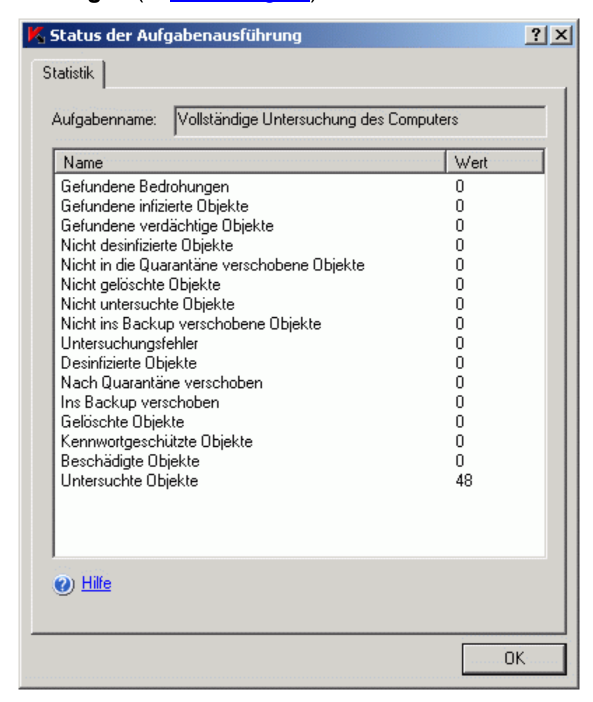


Abbildung 53. Dialogfenster **Status der Aufgabenausführung**

Im Dialogfenster **Status der Aufgabenausführung** werden die folgenden Angaben zu den Objekten angezeigt, die Anti-Virus seit dem Start der Aufgabe bis zum jetzigen Zeitpunkt verarbeitet hat:

- In der Aufgabe **Integritätskontrolle für Anwendungen**:

Feld	Beschreibung
Module mit gestörter Integrität	Anzahl der Modulen mit verletzten Integrität Wenn Module mit verletzter Integrität gefunden worden sind, führen Sie Wiederherstellung des Anti-Virus aus. S. Beschreibung im Dokument *Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition. Installationsanleitung.*
Summe der untersuchten Module	Allgemeine Anzahl der untersuchten Module

- In der Aufgabe **Vollständige Untersuchung des Computers**, **Untersuchung bei Systemstart**, **Untersuchung von Quarantäne-Objekten** und benutzerdefinierten Aufgabe **Virensuche**:

Feld	Beschreibung
Gefundene Bedrohungen	Anzahl der erkannten Bedrohungen. Findet Anti-Virus beispielsweise in fünf Objekten ein Schadprogramm, dann wird der Wert in diesem Feld um eins erhöht.
Gefundene infizierte Objekte	Summe der erkannten infizierten Objekte
Gefundene verdächtige Objekte	Summe der erkannten verdächtigen Objekte
Nicht desinfizierte Objekte	Anzahl der Objekte, die von Anti-Virus nicht desinfiziert wurden, weil: a) Bedrohungsart im Objekt erlaubt keine Desinfizierung; b) dieser Objekttyp kann nicht desinfiziert werden; c) beim Desinfizieren ist ein Fehler aufgetreten

Feld	Beschreibung
Nicht in die Quarantäne verschobene Objekte	Summe der Objekte, die der Anti-Virus in die Quarantäne hätte verschieben müssen, was jedoch aufgrund eines Fehlers nicht gelungen ist, weil beispielsweise nicht genügend Speicherplatz auf dem Datenträger vorhanden war
Nicht gelöschte Objekte	Anzahl der Objekte, die Anti-Virus zu reparieren versucht hat, was aber aus den folgenden Gründen fehlgeschlagen ist, weil beispielsweise der Zugriff auf das Objekt durch eine andere Anwendung gesperrt war
Nicht untersuchte Objekte	Anzahl der im Untersuchungsbereich enthaltenen Objekte, deren Untersuchung durch Anti-Virus fehlgeschlagen ist, z.B. weil der Zugriff auf ein Objekt durch ein anderes Programm gesperrt war
Nicht ins Backup verschobene Objekte	Anzahl der Objekte, die Anti-Virus zu löschen versucht hat, was aber fehlgeschlagen ist, weil beispielsweise der Zugriff auf das Objekt durch eine andere Anwendung gesperrt ist
Untersuchungsfehler	Anzahl der Dateien, deren Kopien Anti-Virus im Backup gespeichert hat
Desinfizierte Objekte	Anzahl der Dateien, deren Kopien Anti-Virus im Backup speichern wollte, was aber aufgrund eines Fehlers nicht gelungen ist
Nach Quarantäne verschoben	Anzahl der Objekte, die Anti-Virus in die Quarantäne verschoben hat
Ins Backup verschoben	Anzahl der Dateien, deren Kopien Anti-Virus im Backup gespeichert hat
Gelöschte Objekte	Erkannte Objekte, die Anti-Virus gelöscht hat
Kennwortgeschützte Objekte	Anzahl der Objekte (zum Beispiel Archive), die Anti-Virus übersprungen hat, weil diese Objekte mit einem Kennwort geschützt sind
Beschädigte Objekte	Summe der Objekte, die der Anti-Virus übersprungen hat, weil deren Format beschädigt war

Feld	Beschreibung
Untersuchte Objekte	Anzahl der Objekte, bei deren Verarbeitung ein Fehler des Anti-Virus aufgetreten ist

KAPITEL 10. UPDATE DER DATENBANKEN UND PROGRAMM-MODULE VON ANTI-VIRUS

In diesem Abschnitt stehen die folgenden Informationen:

- Update der Datenbanken von Anti-Virus (s. Pkt. 10.1 auf S. 151)
- Update der Programm-Module von Anti-Virus (s. Pkt. 10.2 auf S. 152)
- Planung des Updates der Datenbanken und der Programm-Module von Antiviren-Anwendungen im Unternehmen (s. Pkt. 10.3 auf S. 153)
- Beschreibung von Aufgaben zum Update (s. Pkt. 10.4 auf S. 157)
- Einstellung von Aufgaben zum Update:
    - Updatequelle auswählen, Verbindung zur Updatequelle einstellen, Lage des geschützten Servers in Aufgaben zum Update angeben (s. Pkt. 10.5.1 auf S. 159)
    - Einstellen von Parametern der Aufgabe *Update der Programm-Module* (s. Pkt. 10.5.2 auf S. 164)
    - Einstellen von Parametern der Aufgabe *Update-Verteilung* (s. Pkt. 10.5.3 auf S. 166)
- Statistik von Aufgaben zum Update (s. Pkt. 10.6 auf S. 168)
- Rollback von Updates der Anti-Virus-Datenbanken (s. Pkt. 10.7 auf S. 169)
- Rollback von Updates der Programm-Module von Anti-Virus (s. Pkt. 10.8 auf S. 169)

10.1. Update der Anti-Virus-Datenbanken

Die Datenbanken des Anti-Virus, die auf dem geschützten Server gespeichert werden, veralten schnell. Die Viren-Analytiker von Kaspersky Lab entdecken täglich Hunderte neue Bedrohungen, erstellen identifizierende Einträge und übernehmen sie in die Update-Datenbanken. (*Das Update der Datenbanken* ist eine Datei bzw. sind mehrere Dateien mit Einträgen, die Bedrohungen identifizieren, die in der Zeit aufgetreten sind, seit die vorangegangene Datenbank herausgegeben wurde.) Um das Infektionsrisiko auf ein Minimum zu verringern, empfangen Sie regelmäßig Updates der Datenbanken.

In der Grundeinstellung wenn Datenbanken länger, als einer Woche nicht erneuert werden, wird Ereignis *Datenbanken veraltet* ausgelöst, wenn sie länger als zwei Wochen nicht erneuert werden, wird Ereignis *Datenbanken stark veraltet* ausgelöst (Angaben zur Aktualität der Datenbanken werden im Knoten **Statistik** angezeigt, s. Pkt. 13.4 auf S. 223). Sie können eine andere Anzahl der Tage einstellen mit Hilfe von allgemeinen Anti-Virus-Parameter (s. Pkt. 3.2 auf S. 43), wie auch Benachrichtigung des Administrators über diese Ereignisse einstellen (s. Pkt. 15.2 auf S. 237).

Sie können die Datenbanken mit FTP- oder HTTP-*Update-Servern* von Kaspersky Lab aktualisieren oder von anderen Updatequellen, indem Sie die Anti-Virus-Aufgabe **Update der Datenbanken** einsetzen. Details zur Aufgabe **Update der Datenbanken** finden Sie in Pkt. 10.4 auf S. 157.

Sie können Updates auf jeden geschützten Server downloaden oder einen Computer als Sammelpunkt einrichten, so dass auf ihn die Updates geladen und später auf die Server verteilt werden. Wenn Sie außerdem das Programm Kaspersky Administration für die zentralisierte Verwaltung des Computerschutzes im Unternehmen verwenden, können Sie den Administrationsserver von Kaspersky Administration Kit als Sammelpunkt für die Update-Weiterleitung einsetzen. Um die Datenbank ohne deren Übernahme auf den Sammelrechner zu kopieren, verwenden Sie die Aufgabe **Update-Verteilung**. Details zum Parameter finden Sie in Pkt. 10.4 auf S. 157.

Sie können die Aufgaben zum Update manuell oder nach Zeitplan starten. (Näheres zum Einstellen eines Aufgabezeitplans finden Sie in Pkt. 5.7 auf S. 59).

Wenn der Update-Download abbricht oder fehlerhaft verläuft, kehrt Anti-Virus automatisch zur Vorgänger-Version der zuletzt installierten Updates zurück. Sollten die Datenbanken des Anti-Virus beschädigt sein, können Sie selbst ein *Rollback* zu den zuvor installierten Updates ausführen (s. Pkt. 10.7 auf S. 169).

Anmerkung

Wenn Sie keinen Internetzugang haben, können Sie die Updatedateien auf Disketten oder CD-ROMs bei unseren Fachhändlern erhalten. Informationen über den Händler, bei dem Sie Anti-Virus erworben haben, finden Sie in den Eigenschaften des installierten Schlüssels. Außerdem können Sie die Adresse eines Händlers in Ihrer Nähe unter folgenden Telefonnummern bei unserer Zentrale in Moskau erfahren: +7 (495) 797-87-07, +7 (495) 645-79-29 oder +7 (495) 956-87-08 (auf Englisch und Russisch).

10.2. Update der Programm-Module des Anti-Virus

Kaspersky Lab kann Updatepakete für die Programm-Module von Anti-Virus herausgeben. Bei solchen Updates werden dringende (kritische) und geplante Updates unterschieden. *Dringende* Updatepakete beheben Schwachstellen, *geplante* Updates fügen neue Funktionen hinzu oder verbessern vorhandene.

Dringende Updatepakete werden auf den Updateservern von Kaspersky Lab veröffentlicht. Sie können sie automatisch downloaden und installieren, indem Sie die Systemaufgabe **Update der Programm-Module** konfigurieren.

Kaspersky Lab veröffentlicht geplante Update-Pakete nicht auf den Updateservern zum automatischen Installieren; Sie können sich solche Updates von der Kaspersky-Lab-Internetseite laden. Mithilfe der Aufgabe **Update der Programm-Module** können Sie Daten über das Erscheinen von geplanten Anti-Virus-Updates empfangen.

Sie können dringende Updates aus dem Internet auf jeden geschützten Server downloaden oder einen Computer als Sammelpunkt einrichten, so dass auf ihn ohne eine Installation die Updates geladen und später die Updates auf die Server verteilt werden. Um das Update der Datenbanken und ihre Installation zu kopieren und zu speichern, verwenden Sie die Aufgabe **Update-Verteilung**. Details zum Parameter finden Sie in Pkt. 10.4 auf S. 157.

Vor dem Installieren der Updates für die Programm-Module erstellt Anti-Virus Sicherungskopien von den alten Modulen. Wenn das Update der Programm-Module unterbrochen oder fehlerhaft beendet wird, kehrt Anti-Virus automatisch zu den vorher installierten Modul-Versionen zurück. Sie können daneben ein *Rollback der Programm-Module manuell bis zum zuvor installierten Update* ausführen (s. Pkt. 10.8 auf S. 169).

Während der Installation von heruntergeladenen Updates wird der Anti-Virus-Dienst automatisch angehalten und anschließend neu gestartet.

Anmerkung

Wenn Sie keinen Internetzugang haben, können Sie die Updatedateien auf Disketten oder CD-ROMs bei unseren Fachhändlern erhalten. Informationen über den Händler, bei dem Sie Anti-Virus erworben haben, finden Sie in den Eigenschaften des installierten Schlüssels. Außerdem können Sie die Adresse eines Händlers in Ihrer Nähe unter folgenden Telefonnummern bei unserer Zentrale in Moskau erfahren: +7 (495) 797-87-07, +7 (495) 645-79-29 oder +7 (495) 956-87-08 (auf Englisch und Russisch).

10.3. Planung des Updates der Datenbanken und der Programm-Module von Antiviren-Anwendungen im Unternehmen

Die Auswahl der Updatequelle in den Aufgaben zum Update ist davon abhängig, nach welchem Schema die Datenbanken und Programm-Module der Antiviren-Anwendungen in Ihrem Unternehmen aktualisiert werden.

Sie können die Datenbanken und Module von Anti-Virus auf den geschützten Servern nach folgenden Schemata aktualisieren:

- Download von Updates direkt aus dem Internet auf jeden geschützten Server (**Schema 1**)
- Download von Updates aus dem Internet auf einen ausgewählten Computer und anschließende Verteilung auf die übrigen Server

  Als Verteiler kann ein beliebiger Computer dienen, auf dem installiert ist:

  - Anti-Virus (einer der geschützten Server) (**Schema 2**)

    oder

  - Administrationsserver von Kaspersky Administration Kit (**Schema 3**)

  Das Update über einen Computer, der als Verteiler funktioniert, erlaubt nicht nur die Einsparung von Internet-Datenverkehr, sondern bietet auch zusätzliche Sicherheit für die Server.

Die genannten Update-Schemata werden im Folgenden beschrieben.

Schema 1. Update direkt aus dem Internet

Legen Sie auf jedem geschützten Server die Aufgabe **Update der Datenbanken** (**Update der Programm-Module**) an. Geben Sie als Updatequelle die Kaspersky-Lab-Updateserver an. Passen Sie den Zeitplan der Aufgabe an.

Als Updatequelle können auch andere HTTP- oder FTP-Server gewählt werden, auf denen ein Ordner mit den Updatedateien vorhanden ist.

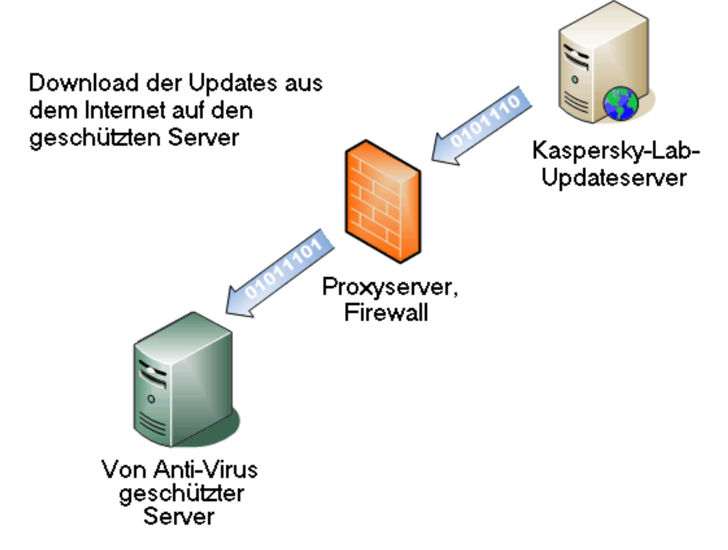


Abbildung 54. Update direkt aus dem Internet

Schema 2. Update über einen der geschützten Server

Das Update nach diesem Schema (s. Abbildung 55) umfasst folgende Schritte:

Schritt 1. Kopieren der Updates auf den ausgewählten geschützten Server

Passen Sie auf dem als Verteiler ausgewählten Server die Aufgabe **Update-Verteilung** an. Geben Sie dabei als Updatequelle die Kaspersky-Lab-Updateserver an. Legen Sie als Ordner, in dem die Updates gespeichert werden sollen, einen gemeinsamen Ordner fest.

Unter Verwendung dieser Aufgabe können Sie nicht nur Updates für die geschützten Server empfangen, sondern auch für Rechner im lokalen Netzwerk, auf denen andere Anwendungen von Kaspersky Lab der Version 6.0

(zum Beispiel Kaspersky Anti-Virus 6.0 for Windows Workstations) installiert sind.

Schritt 2. Verteilung der Updates auf die übrigen geschützten Server

Passen Sie auf jedem der geschützten Server die Aufgabe **Update der Datenbanken** (**Update der Programm-Module**) an. Geben Sie dabei als Updatequelle den Ordner auf dem Laufwerk des ausgewählten Rechners an, in den die Updates kopiert werden.

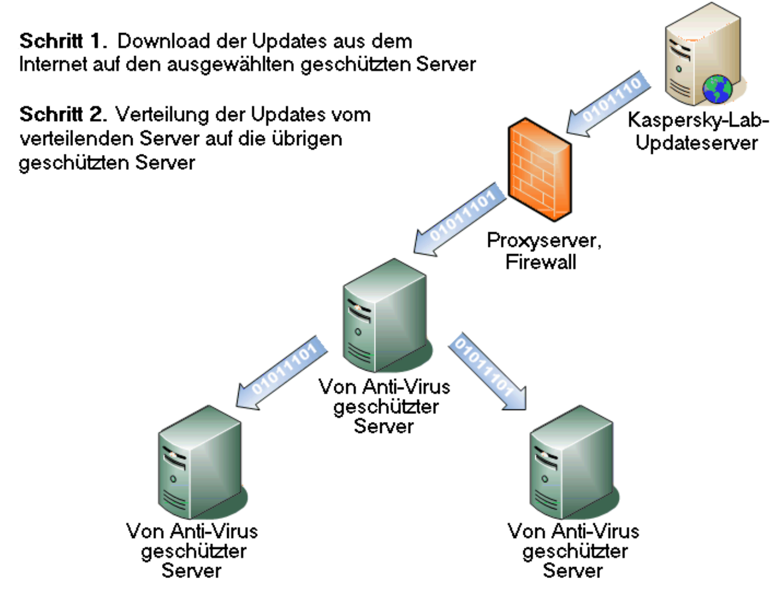


Abbildung 55. Update über einen der geschützten Server

Schema 3. Update-Download über den Administrationsserver von Kaspersky Administration Kit

Wenn Sie das Programm Kaspersky Administration Kit für die zentrale Verwaltung des Schutzes von Computern einsetzen, können Sie Updates über den Administrationsserver von Kaspersky Administration Kit downloaden (s. Abbildung 56).

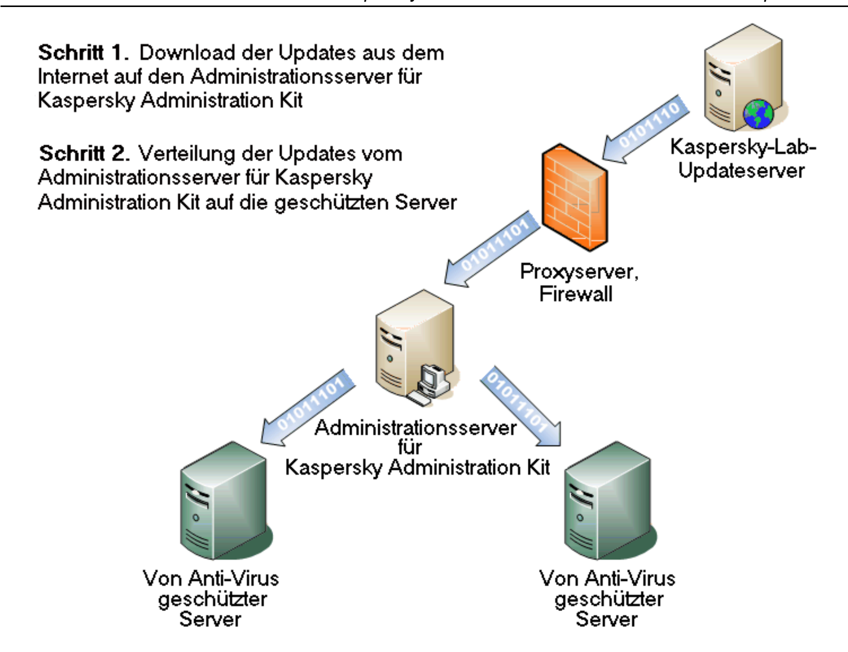


Abbildung 56. Update über den Administrationsserver von Kaspersky Administration Kit

Das Update nach diesem Schema umfasst folgende Schritte:

Schritt 1. Update-Download von einem Kaspersky-Lab-Updateserver auf den Administrationsserver von Kaspersky Administration Kit

Passen Sie die globale Aufgabe **Update-Download durch Administrationsserver** an. Geben Sie dabei als Updatequelle die Kaspersky-Lab-Updateserver an.

Sie können nicht nur Updates für die geschützten Server empfangen, sondern auch für Rechner im lokalen Netzwerk, auf denen andere Anwendungen von Kaspersky Lab der Version 6.0 (zum Beispiel Kaspersky Anti-Virus 6.0 for Windows Workstations) installiert sind.

Schritt 2. Verteilung der Updates auf die geschützten Server

Zur Update-Verteilung auf die geschützten Server stehen folgende Varianten zur Verfügung:

- Passen Sie die globale Aufgabe zum Update der Anti-Virus-Datenbanken (Programm-Module) auf dem Administrationsserver von Kaspersky Administration Kit so an, dass die Update-Verbreitung auf die geschützten Server erfolgt. Geben Sie im Zeitplan der Aufgabe die Starthäufigkeit **Aufgabe bei Update-Download durch Administrati-**

onsserver starten an. Der Administrationsserver startet die Aufgabe jedes Mal, wenn er Updates empfängt (Diese Variante wird empfohlen).

Stellen Sie den Zeitplan der Aufgabe ein. Für eine Aufgabe, die auf der Administrationskonsole erstellt wird, können Sie die Startfrequenz **Nach Update-Download durch Administrationsserver** angeben. Die Aufgabe wird jedes Mal gestartet, sobald der Administrationsserver Updates empfängt.

Hinweis

Die Startfrequenz **Nach Update-Download durch Administrationsserver** kann in der Anti-Virus-MMC-Konsole nicht angegeben werden.

- Passen Sie auf jedem geschützten Server die Aufgabe **Update der Datenbanken** (**Update der Programm-Module**) an. Geben Sie dabei als Updatequelle den Administrationsserver von Kaspersky Administration Kit an. Stellen Sie den Zeitplan der Aufgabe ein.

Wenn Sie den Einsatz des Administrationsservers von Kaspersky Administration Kit zum Verbreiten der Updates planen, installieren Sie zuerst auf jedem geschützten Server die Programmkomponente Administrationsagent, die zum Lieferumfang des Programms Kaspersky Administration Kit gehört. Er sorgt auf dem geschützten Server für die Interaktion zwischen dem Administrationsserver und dem Anti-Virus. Details zum Administrationsagenten und dessen Einstellung mit dem Programm Kaspersky Administration Kit finden Sie im Dokument *Kaspersky Administration Kit. Administratorhandbuch*.

10.4. Aufgaben zum Update

Im Anti-Virus sind vier Systemaufgaben für Update vordefiniert: **Update der Datenbanken**, **Update der Programm-Module**, **Update-Verteilung** und **Rollback des Datenbank-Updates** (s. Abbildung 57).

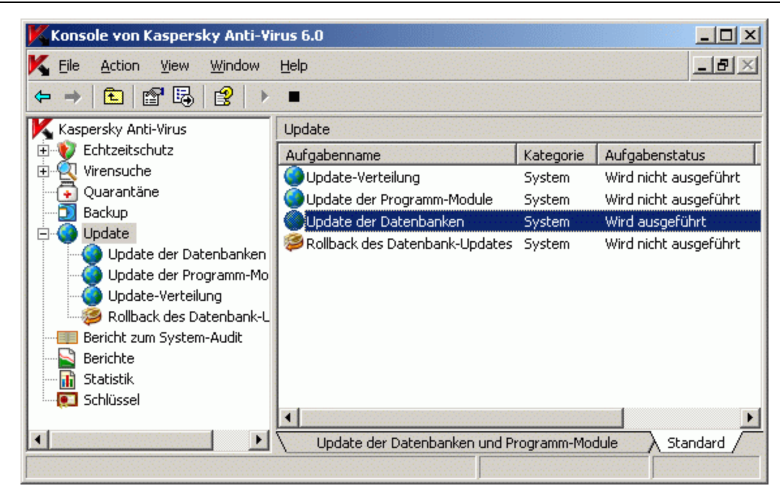


Abbildung 57. Aufgaben zum Update im Fenster Anti-Virus-Konsole

Update der Programm-Datenbanken

Anti-Virus kopiert die Datenbanken aus der Updatequelle auf den geschützten Server und wechselt sofort zu ihnen, wenn Aufgaben des Echtzeitschutzes und Virensuche ausgeführt werden sollen.

Standardmäßig startet Anti-Virus die Aufgabe **Update der Datenbanken** jede Stunde. Er stellt eine Verbindung zur Updatequelle her, einem Update-Server von Kaspersky Lab, indem er automatisch die Parameter des Proxyserver im Netzwerk ermittelt und die Authentifizierung beim Zugriff auf den Proxyserver nicht prüft.

Update der Programm-Module

Anti-Virus kopiert die Updates seiner Programm-Module aus der Updatequelle auf den geschützten Server und installiert die Module. Zur Übernahme der installierten Programm-Module muss möglicherweise der Computer und/oder Anti-Virus neu gestartet werden.

Jede Woche startet Anti-Virus am Freitag um 16.00 Uhr (Uhrzeit in dem Format, das in den Regionsoptionen des geschützten Servers eingestellt ist) die Aufgabe **Update der Programm-Module**, um nur das Vorhandensein von kritischen und geplanten Updates der Anti-Virus-Module zu prüfen, ohne sie zu kopieren.

Update-Verteilung

Anti-Virus lädt die Dateien für das Update der Datenbanken und Programm-Module und speichert sie in dem angegebenen Netzwerkordner oder lokalen Ordner, ohne sie zu übernehmen.

Rollback des Datenbank-Updates

Anti-Virus kehrt zu den Datenbanken der zuvor installierten Updates zurück.

Wie die Aufgaben zum Update eingestellt werden, finden Sie in Pkt. 10.5 auf S. 159.

Anmerkung

Sie können Aufgaben zum Update beenden, können Sie allerdings nicht anhalten.

Wie die Aufgaben im Anti-Virus verwaltet werden, finden Sie in Pkt. 5.6 auf S. 58.

10.5. Aufgaben zum Update einstellen

In diesem Abschnitt wird beschrieben, wie die folgenden Aktionen in Aufgaben zum Update ausgeführt werden:

- Updatequelle auswählen, Verbindung zur Updatequelle einstellen, Standort des geschützten Servers für Optimierung des Update-Downloads angeben (Parameter sind in jeder Aufgaben zum Update enthalten) (s. Pkt. 10.5.1 auf S. 159)
- Einstellen von Parametern der Aufgabe *Update der Programm-Module* (s. Pkt. 10.5.2 auf S. 164)
- Einstellen von Parametern der Aufgabe *Update-Verteilung* (s. Pkt. 10.5.3 auf S. 166)

10.5.1. Updatequelle auswählen, Verbindung zur Updatequelle und Regionsoptionen einstellen

In jeder Aufgabe zum Update können Sie eine oder mehrere Updatequellen angeben, die Verbindung mit den Quellen einstellen und den Standort des geschützten Servers festlegen, um den Update-Download (Regionsoptionen) zu optimieren.

Um die Update-Parameter einzustellen, machen Sie Folgendes:

1. Gehen Sie in der Konsolenstruktur auf **Update**.

2. Öffnen Sie das Kontextmenü mit einem Rechtsklick auf die Aufgabe zum Update, in der Sie die Updatequelle einstellen wollen, und gehen Sie auf **Eigenschaften**.

   Auf den Registerkarten des Dialogfensters **Eigenschaften: <Aufgabe>** konfigurieren Sie die gewünschten Update-Parameter je nach Ihren Wünschen.

3. Auf der Registerkarte **Allgemein** (s. Abbildung 58) wählen Sie die Quelle aus, aus der Sie Updates downloaden wollen (Details zum Parameter finden Sie in Pkt. B.5.1 auf S. 419).

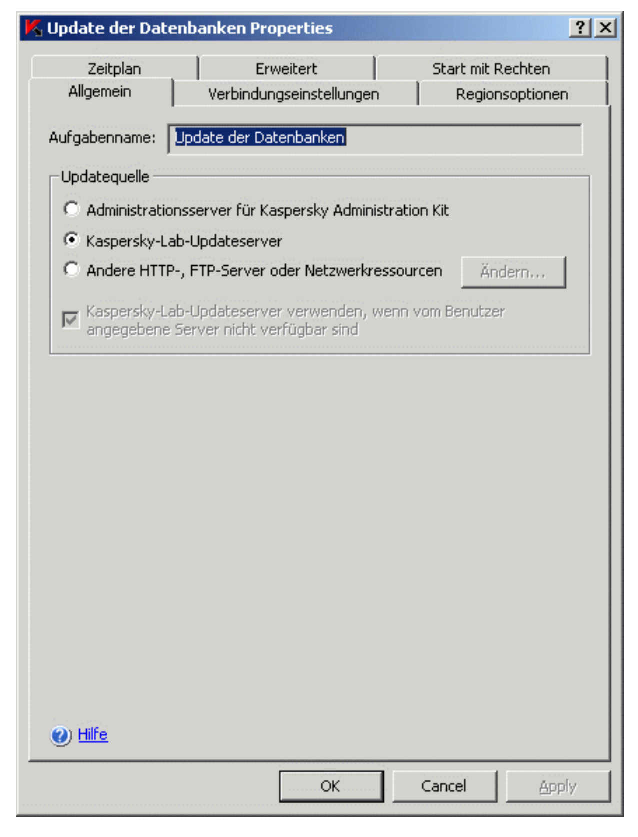


Abbildung 58. Dialogfenster **Eigenschaften: <Aufgabe>**, Registerkarte **Allgemein**

4. Wenn Sie **Andere HTTP-, FTP-Server oder Netzwerkressourcen** gewählt haben, fügen Sie eine oder mehrere benutzerdefinierte Updatequellen hinzu. Um eine Quelle anzugeben, klicken Sie auf die Schaltfläche **Ändern** und im Dialogfenster **Updateserver** (s. Abbildung 59) kli-

cken Sie auf die Schaltfläche **Hinzufügen** und im Eingabefeld geben Sie die Adresse des Ordners mit den Update-Dateien auf dem FTP- oder HTTP-Server an. Den lokalen Ordner oder den Netzwerkordner geben Sie im UNC-Format (Universal Naming Convention) an. Klicken Sie auf die Schaltfläche **OK**.

Sie können hinzugefügte benutzerdefinierte Quelle aktivieren oder deaktivieren: Um eine hinzugefügte Quelle zu deaktivieren, entfernen Sie das Häkchen neben der Quelle in der Liste. Um die Quelle zu aktivieren, setzen Sie das Häkchen neben der Quelle.

Um die Reihenfolge zu ändern, die Anti-Virus die benutzerdefinierten Quellen durchsucht, verschieben Sie mithilfe der Schaltflächen **Aufwärts** und **Abwärts** die gewünschte Quelle an den Anfang oder an das Ende der Liste, je nach dem, ob die Quelle früher oder später angesteuert werden soll.

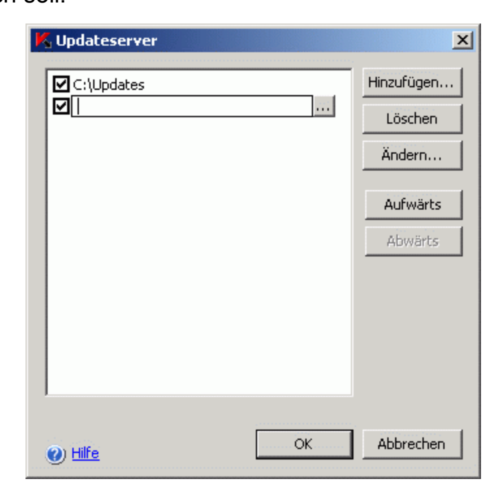


Abbildung 59. Hinzufügen von benutzerdefinierten Updatequellen

Um den Pfad zur Quelle zu ändern, markieren Sie die Quelle in der Liste und klicken auf die Schaltfläche **Ändern**, nehmen Sie die gewünschten Änderungen im Eingabefeld vor und klicken Sie auf den Button **OK**

Um die Vorlage zu löschen, markieren Sie sie in der Liste und klicken Sie auf die Schaltfläche **Löschen**. Die Quelle wird aus der Liste entfernt.

5. Um für den Update-Download die Update-Server von Kaspersky Lab zu verwenden, falls nicht auf die benutzerdefinierten Quellen zugegriffen werden kann, setzen Sie das Häkchen im Kontrollkästchen **Kaspersky-**

Lab-Updateserver verwenden, wenn vom Benutzer angegebene Server nicht verfügbar sind.

6. Auf der Registerkarte **Verbindungseinstellungen** (s. Abbildung 60) stellen Sie die Verbindung mit der Updatequelle ein.

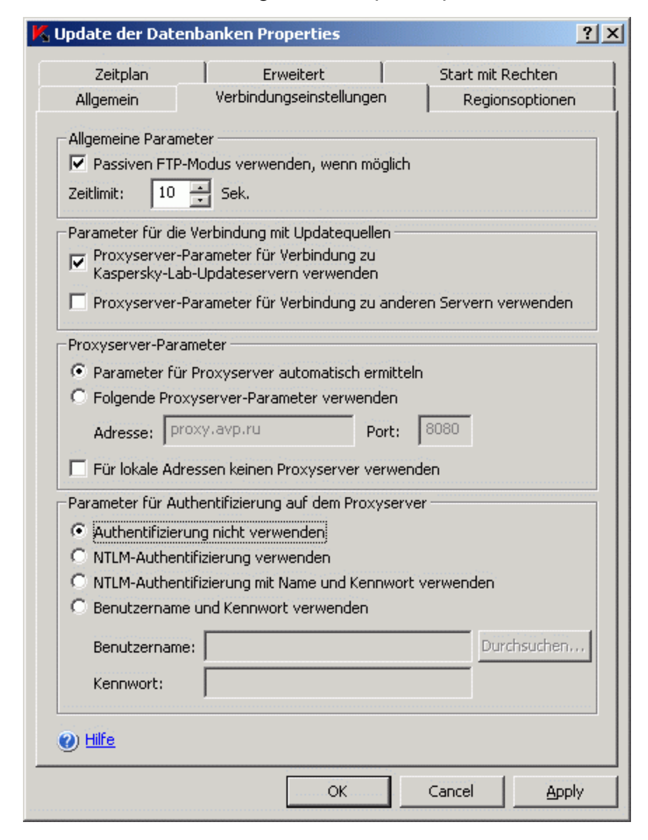


Abbildung 60. Dialogfenster **Eigenschaften: <Aufgabe>**, Registerkarte **Verbindungseinstellungen**

Führen Sie die folgenden Aktionen aus:

- Geben Sie den Modus des FTP-Servers für die Verbindung mit dem geschützten Server an (s. Pkt. B.5.2 auf S. 421).
- Bei Bedarf ändern Sie die Wartezeit für die Verbindung mit der Updatequelle (s. Pkt. B.5.3 auf S. 421).

- Wenn für den Update-Download von einer angegebenen Quelle auf einen Proxyserver zugegriffen werden muss, beschreiben Sie die Parameter des Proxyservers:
  - Zugriff auf den Proxy-Server bei Verbindung mit verschiedenen Updatequellen (s. Pkt. B.5.4.1 auf S. 422)
  - Adresse des Proxy-Servers (s. Pkt. B.5.4.2 auf S. 423)
  - Authentifizierungsmethode bei Zugriff auf Proxy-Server (s. Pkt. B.5.4.3 auf S. 424)

7. Auf der Registerkarte **Regionsoptionen** (s. Abbildung 61) wählen Sie das Land, in dem der geschützte Server steht, aus der Liste **Standort** aus (Details zum Parameter finden Sie in Pkt. B.5.5 auf S. 425).

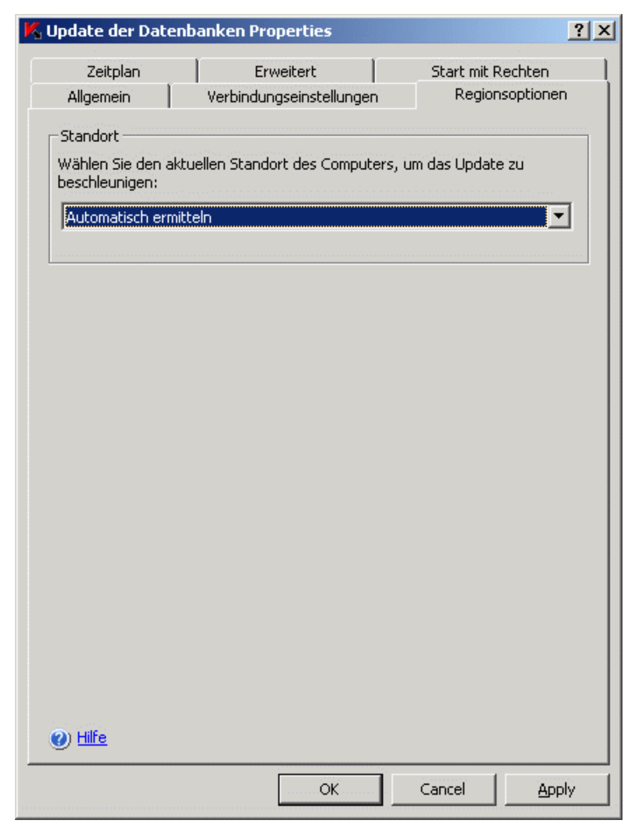


Abbildung 61. Dialogfenster **Eigenschaften: <Aufgabe>**, Registerkarte **Regionsoptionen**

8. Nachdem Sie die gewünschten Parameter eingestellt haben, klicken Sie auf **OK**, um die Änderungen zu speichern.

10.5.2. Parameter der Aufgabe *Update der Programm-Module* einstellen

*Um die Parameter für die Aufgabe **Update der Programm-Module** einzustellen, machen Sie Folgendes:*

1. Gehen Sie in der Konsolenstruktur auf den Knoten **Update**.
2. Öffnen Sie das Kontextmenü für die Aufgabe **Update der Programm-Module** und gehen Sie auf **Eigenschaften**.
3. Geben Sie im Dialogfenster **Eigenschaften: Update der Programm-Module** die Updatequelle und die Parameter für die Verbindung mit der Quelle an (s. Anleitung in Pkt. 10.5.1 auf S. 159).
4. Wählen Sie auf der Registerkarte **Allgemein** (s. Abbildung 62), ob die Updates kopiert und installiert werden sollen oder ob nur das Vorhandensein von Updates geprüft werden soll (Details zum Parameter s. Pkt. B.5.6.1 auf S. 426).

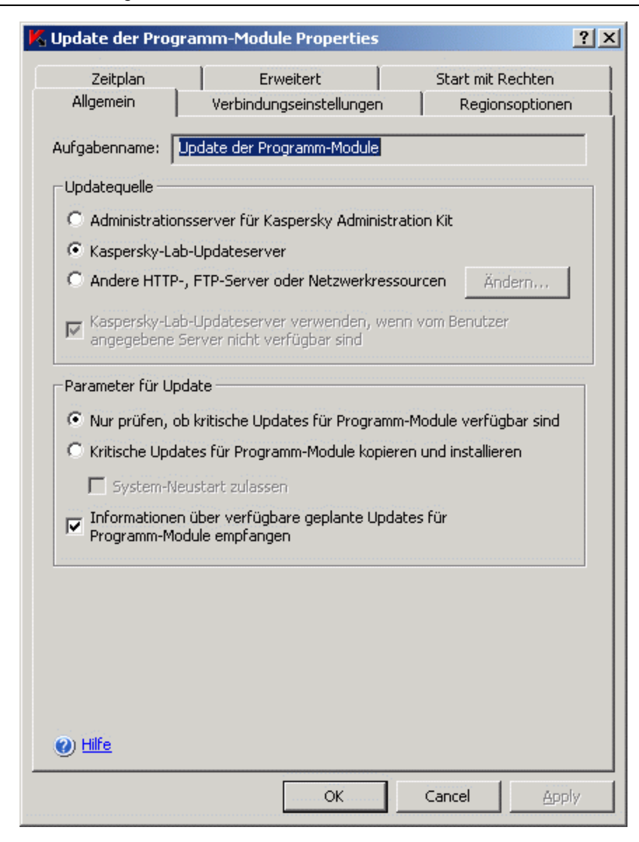


Abbildung 62. Dialogfenster **Eigenschaften: Update der Programm-Module**, Registerkarte **Allgemein**

5. Damit Anti-Virus nach dem Abschluss der Aufgabe den Server automatisch neu startet, wenn der Neustart zum Übernehmen von installierten Programm-Modulen erforderlich ist, aktivieren Sie das Kontrollkästchen **System-Neustart zulassen**.

6. Wenn Sie Daten über die Veröffentlichung von geplanten Updates für Anti-Virus-Module downloaden wollen, setzen Sie das Häkchen im Kontrollkästchen **Informationen über verfügbare geplante Updates für Programm-Module empfangen**.

   Kaspersky Lab veröffentlicht geplante Update-Pakete nicht auf den Updateservern zum automatischen Updaten, sondern Sie laden sich solche Updates von der Kaspersky-Lab-Internetseite. Sie können einstellen, den Administrator über das Ereignis *Geplante Update für Anti-*

Virus-Module sind verfügbar zu benachrichtigen, so dass er die Adresse unserer Internetseite erfährt, von der Sie die geplanten Updates downloaden können (Details zur Einstellung von Benachrichtigungen finden Sie in Pkt. 15.2 auf S. 237).

7. Klicken Sie auf **OK**, um die Änderungen zu speichern.

10.5.3. Parameter für die Aufgabe *Update-Verteilung* einstellen

Um die Parameter für die Aufgabe ***Update-Verteilung*** *einzustellen, machen Sie Folgendes:*

1. Gehen Sie in der Konsolenstruktur auf den Knoten **Update**.
2. Öffnen Sie das Kontextmenü für die Aufgabe **Update-Verteilung** und gehen Sie auf **Eigenschaften**.
3. Geben Sie im Dialogfenster **Eigenschaften: Update-Verteilung** (s. Abbildung 63) die Updatequelle und die Parameter für die Verbindung mit der Quelle an (s. Anleitung in Pkt. 10.5.1 auf S. 159).

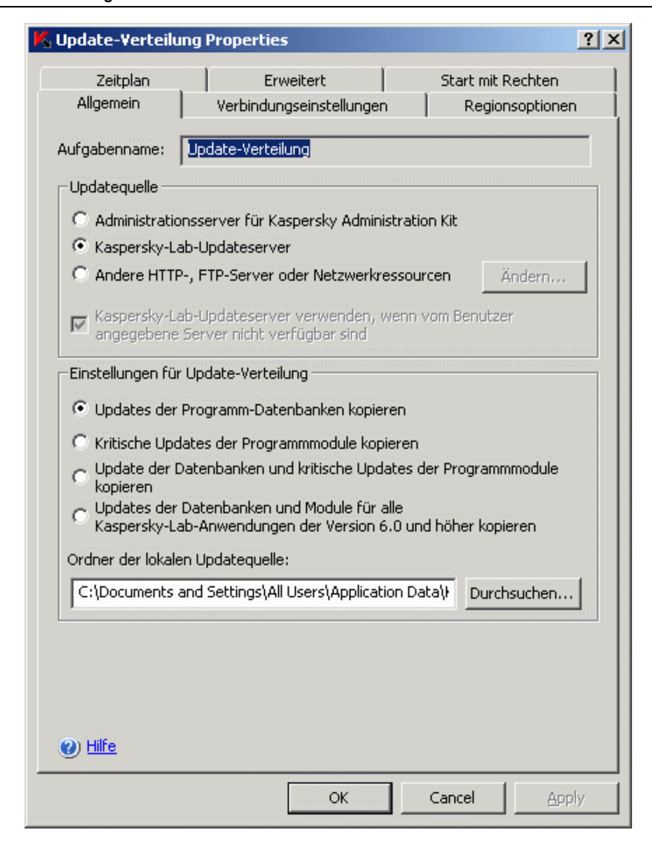


Abbildung 63. Dialogfenster **Eigenschaften: Update-Verteilung**, Registerkarte **Allgemein**

4. Geben Sie auf der Registerkarte **Allgemein** die Zusammensetzung der Updates an, die in den vorgegebenen Ordner kopiert werden (Details zum Parameter finden Sie in Pkt. B.5.7.1 auf S. 428).

5. Geben Sie einen lokalen Ordner oder einen Netzwerkordner an, in den Anti-Virus die geladenen Updates speichert (Details zum Parameter finden Sie in Pkt. B.5.7.2 auf S. 429).

6. Klicken Sie auf **OK**, um die Änderungen zu übernehmen.

10.6. Statistik von Aufgaben zum Update

Solange eine Aufgabe zum Update ausgeführt wird, können Sie Detailinformationen zum Umfang der Daten in Echtzeit anzeigen lassen, die seit dem Aufgabenstart bis jetzt verarbeitet wurde, eine *Aufgabenstatistik*.

Information in dem Dialogfenster **Statistik** wird sichtbar**,** wenn Sie die Aufgabe anhalten. Nach dem Abschluss oder Beenden der Aufgabe steht die Aufgabenstatistik über die Ausführung der Aufgabe im Knoten **Berichte** (s. Pkt. 13.2.4 auf S. 210) zugängig sein.

Um eine Statistik für eine Aufgabe zum Update anzuzeigen, machen Sie Folgendes:

1. Klappen Sie in der Konsolenstruktur den Knoten **Update** auf.
2. Öffnen Sie das Kontextmenü für die gewünschte Aufgabe und gehen Sie auf **Statistik anzeigen**.

Im Dialogfenster **Status der Aufgabenausführung** für die Aufgaben **Update der Programm-Datenbanken** und **Update-Verteilung** wird das Datenvolumen angezeigt, das Anti-Virus bis jetzt geladen hat (**Empfangene Daten**).

Im Dialogfenster **Status der Aufgabenausführung** für die Aufgabe **Update der Programm-Module** werden die folgenden Informationen angezeigt:

Feld	Beschreibung
Erhaltene Daten	Gesamtvolumen der erhaltenen Daten
Kritische Updates sind verfügbar	Menge der kritischen Updates, die zur Installation bereitstehen
Geplante Updates sind verfügbar	Menge der geplanten Updates, die zur Installation bereitstehen
Fehler bei Update-Übernahme	Wenn dieser Wert von Null abweicht, wurden Updates nicht übernommen. Sie können im Detailprotokoll feststellen, für welches Update beim Übernehmen ein Fehler aufgetreten ist.

10.7. Rollback von Updates der Anti-Virus-Datenbanken

Anti-Virus legt, bevor er ein Update der Datenbanken übernimmt, Sicherungskopien von den alten Datenbanken an. Wenn der Update-Download abbricht oder fehlerhaft verläuft, kehrt Anti-Virus automatisch zu den Datenbanken mit den zuvor installierten Updates zurück.

Wenn bei Ihnen nach dem Update ein Problem auftritt, können Sie die Datenbanken bis zur vorangegangenen Version der installierten Updates manuell rückgängig machen, indem Sie die Aufgabe **Rollback des Datenbank-Update** starten.

10.8. Rollback von Update der Programm-Module

Vor der Übernahme der Updates der Programm-Module erstellt Anti-Virus Sicherungskopien von den alten Modulen. Wenn das Modul-Update abbricht oder fehlerhaft verläuft, kehrt Anti-Virus automatisch zur Vorgänger-Version der zuletzt installierten Updates zurück.

Sie können ein *manuelles Rollback der Programm-Module* bis zum zuvor installierten Update ausführen.

*Um ein manuelles Rollback der Programm-Module auszuführen, verwenden Sie die Verwaltungskomponente von Microsoft Windows **Programme ändern und entfernen**.*

KAPITEL 11. ISOLIERUNG VON VERDÄCHTIGEN OBJEKTEN. ISOLIEREN IN QUARANTÄNE

In diesem Kapitel stehen die folgenden Informationen:

- Isolieren von verdächtigen Objekten (s. Pkt. 11.1 auf S. 170)
- Objekte in der Quarantäne anzeigen, sortieren und filtern (s. Pkt. 11.2 auf S. 171)
- Objekte in Quarantäne untersuchen (bei Bedarf oder automatisch, nach jedem Update der Datenbanken) (s. Pkt. 11.3 auf S. 175)
- Objekte aus Quarantäne wiederherstellen (s. Pkt. 11.4 auf S. 177)
- Objekte manuell in Quarantäne verschieben (s. Pkt. 11.5 auf S. 181)
- Objekte aus Quarantäne löschen (s. Pkt. 11.6 auf S. 182)
- Verdächtige Objekte aus Quarantäne zur Analyse in Virenlabor einschicken (s. Pkt. 11.7 auf S. 183)
- Einstellung der Quarantäne-Parameter (s. Pkt. 11.8 auf S. 185)
- Statistik für Quarantäne

Parameterbeschreibung für Quarantäne ist in Pkt. B.6 auf S. 430 beschrieben.

11.1. Isolierung von verdächtigen Objekten

Anti-Virus isoliert Objekte, die er als verdächtig erkennt, indem er sie in die *Quarantäne* verschiebt, sie von ihrem ursprünglichen Speicherplatz in einen speziellen Ordner umlagert, in dem er sie aus Sicherheitsgründen verschlüsselt aufbewahrt (Details dazu, wie Anti-Virus Objekt als verdächtig einstuft, finden Sie in Pkt. 1.1.3 auf S. 19).

11.2. Objekte in Quarantäne anzeigen

Sie können in der Quarantäne liegende Objekte im Knoten **Quarantäne** der Anti-Virus-Konsole anzeigen lassen.

*Um die Objekte in der Quarantäne anzuzeigen, gehen Sie in der Konsolenstruktur auf den Knoten **Quarantäne** (s. Abbildung 64).*

Um ein gewünschtes Objekt in der Liste der Quarantäne-Objekte zu suchen, können Sie die Objekte sortieren (s. Pkt. 11.2.1 auf S. 173) oder filtern (s. Pkt. 11.2.2 auf S. 174).

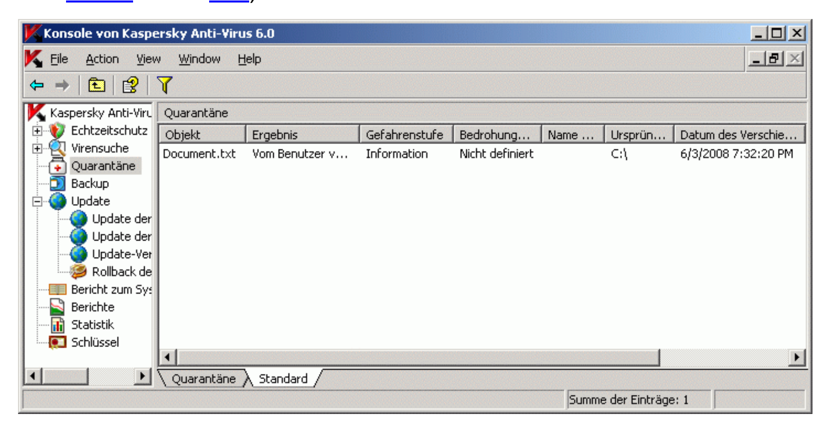


Abbildung 64. Informationen zu Quarantäne-Objekten im Knoten **Quarantäne**

Im Ergebnisfenster werden die folgenden Informationen zu jedem Quarantäne-Objekt angezeigt:

Tabelle 7. Informationen zu den Quarantäne-Objekten

Feld	Beschreibung
Objekt	Name des in die Quarantäne verschobenen Objektes
Ergebnis	Status des Objektes in der Quarantäne kann folgende Werte haben: • **Warnung**. Das Objekt wurde mit der heuristischen Analysemethode als verdächtig eingestuft. • **Verdächtig**. Das Objekt wurde als verdächtig eingestuft. Es wurde eine partielle Übereinstimmung von Codebe-

Feld	Beschreibung
	standteilen des Objektes mit Codebestandteilen von einer bekannten Bedrohung festgestellt. • **Infiziert**. Das Objekt wurde als infiziert eingestuft. Es wurde eine komplette Übereinstimmung von Codebestandteilen des Objektes mit Codebestandteilen von einer bekannten Bedrohung festgestellt. • **Verarbeitungsfehler**. Anti-Virus hat das Objekt in die Quarantäne als verdächtig verschoben oder Sie haben das Objekt von Hand in die Quarantäne verschoben, aber bei der Quarantäne-Untersuchung anhand von aktualisierten Datenbanken hat Anti-Virus das Objekt als nicht infiziert eingestuft. • **Desinfiziert**. Anti-Virus hat das Objekt in die Quarantäne als verdächtig verschoben oder Sie haben das Objekt von Hand in die Quarantäne verschoben, aber bei der Quarantäne-Untersuchung anhand von aktualisierten Datenbanken hat Anti-Virus das Objekt als infiziert eingestuft und es desinfiziert. Sie können das Objekt ohne Bedenken wiederherstellen. • **Vom Benutzer verschoben**. Das Objekt ist vom Benutzer in die Quarantäne verschoben worden.
Gefahrenstufe	Die Gefahrenstufe zeigt an, wie gefährlich das Objekt für den Server ist. Die Gefahrenstufe hängt vom Bedrohungstyp im Objekt ab und kann die folgenden Werte annehmen (Details zu den Bedrohungstypen finden Sie in Pkt. 1.1.2 auf S. 15): • **Hoch**. Das Objekt könnte eine Bedrohung der Art *Netzwerkwürmer*, *klassische Viren*, *Trojanische Programme* oder eine Bedrohung eines nicht bestimmbaren Typs (zu diesem Typ gehören neue Viren, die zurzeit noch nicht einem bekannten Typ zugeordnet werden können) enthalten. • **Mittel**. Das Objekt könnte eine Bedrohung des Typs *diverse schädliche Programme*, *Adware* oder *Pornware* enthalten. • **Niedrig**. Das Objekt könnte eine Bedrohung des Typs *potentiell gefährliche Programme* enthalten. • **Informativ**. Das Objekt ist vom Benutzer in die Quarantäne verschoben worden.

Feld	Beschreibung
Bedrohungstyp	Die Bedrohungsart nach der Klassifizierung von Kaspersky Lab gehört zur vollständigen Bezeichnung einer Bedrohung, die Anti-Virus meldet, nachdem er ein Objekt als verdächtig oder infiziert eingestuft hat.
Name der Bedrohung	Der Name einer Bedrohung nach der Klassifizierung von Kaspersky Lab gehört zur vollständigen Bezeichnung einer Bedrohung in einem Objekt, die Anti-Virus meldet, nachdem er ein Objekt als verdächtig oder infiziert eingestuft hat. Sie können den vollen Namen der im Objekt gefundenen Bedrohung im Detailbericht über die über Aufgabenausführung finden (Knoten **Berichte**).
Datum des Verschiebens	Datum der Verschiebung des Objektes in die Quarantäne
Ursprünglicher Pfad	Vollständiger Pfad zum ursprünglichen Speicherplatz des Objektes, beispielsweise zum Ordner, aus dem das Objekt in den Quarantäne-Ordner übertragen wurde, zur Archiv-Datei oder zur *pst*-Datei in einer Mail-Datenbank.
Größe	Objektgröße
Benutzername	Die Spalte kann folgende Daten enthalten: • Wenn das Objekt von Anti-Virus in der Aufgabe **Echtzeitschutz für Dateien** isoliert wurde – Name des Benutzerkontos, mit dessen Rechten die Anwendung auf das Objekt zugegriffen hat, als es abgefangen wurde. • Wenn das Objekt von Anti-Virus in einer Aufgabe zur Virensuche isoliert wurde – Name des Benutzerkontos, mit dessen Rechten die Aufgabe ausgeführt wurde. • Wenn der Benutzer das Objekt manuell in die Quarantäne verschoben hat – Name seines Benutzerkontos.

11.2.1. Sortieren von Objekten in Quarantäne

Standardmäßig werden die Objekte in der Liste mit den Quarantäne-Objekten nach dem Verschiebedatum in umgekehrter chronologischer Reihenfolge sortiert. Um das gewünschte Objekt zu finden, können Sie die Objekte nach dem

Spalteninhalt und den Objektinformationen sortieren lassen. Das Sortierergebnis wird gespeichert, wenn Sie den Knoten **Quarantäne**verlassen oder wenn Sie die Anti-Virus-Konsole mit Speichern in der *msc*-Datei schließen und sie wieder aus dieser Datei wieder öffnen.

Um Objekte zu sortieren, machen Sie Folgendes:

1. Gehen Sie in der Konsolenstruktur auf den Knoten **Quarantäne**.
2. Im Ergebnisfenster klicken Sie in der Ereignisliste auf den Spaltenkopf, nach dessen Inhalt Sie die Listenobjekte sortieren wollen.

11.2.2. Objekte in Quarantäne filtern

Um ein Objekt in der Quarantäne zu suchen, können Sie die Objekte in der Liste filtern, das heißt nur Objekte anzuzeigen, die den von Ihnen eingegebenen Filterkriterien (Filtern) entsprechen. Das Filterergebnis wird gespeichert, wenn Sie den Knoten **Quarantäne** verlassen oder wenn Sie die Anti-Virus-Konsole mit Speichern in der *msc*-Datei schließen und sie wieder aus dieser Datei wieder öffnen.

Um einen oder mehrere Filter einzugeben, machen Sie Folgendes:

1. In der Konsolenstruktur öffnen Sie das Kontextmenü für den Knoten **Quarantäne** und gehen Sie auf den Eintrag **Filter**.

   Es öffnet sich das Dialogfenster **Filterparameter** (s. Abbildung 65).

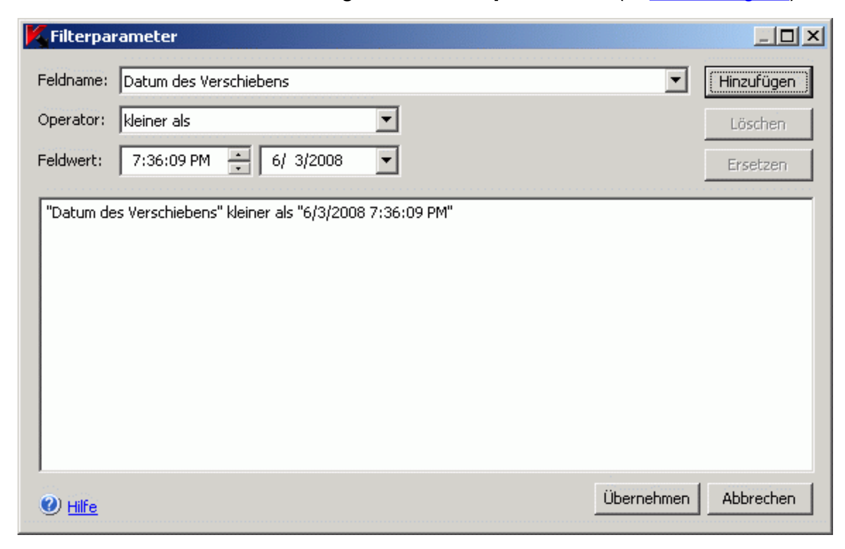


Abbildung 65. Dialogfenster **Filterparameter**

2. Um einen Filter hinzuzufügen, machen Sie Folgendes:

   a) In der Liste **Feldname** wählen Sie ein Feld aus, mit dem der Filterwert verglichen wird.

   b) In der Liste **Operator** wählen Sie die Filterbedingung aus. Die Bedingungswerte für das Filtern in der Liste können sich voneinander unterscheiden, je nach dem, welchen Wert Sie in der Liste **Feldname** ausgewählt haben.

   c) Im Feld **Feldwert** geben einen Filterwert ein oder markieren einen Filterwert in der Liste.

   d) Klicken Sie auf die Schaltfläche **Hinzufügen**.

      Der hinzugefügte Filter wird in der Filterliste im Fenster **Filterparameter** dargestellt. Wiederholen Sie diese Vorgänge für jeden Filter, den Sie hinzufügen wollen. Wenn Sie mehrere Filter eingeben, werden sie mit einem logischen **UND** verknüpft.

- Um einen Filter zu löschen, markieren Sie den zu entfernenden in der Filterliste und klicken Sie auf die Schaltfläche **Löschen**.

- Um einen Filter zu bearbeiten, markieren Sie ihn in der Filterliste des Dialogfensters **Filterparameter**, ändern Sie dann die gewünschten Werte in den Feldern **Feldname**, **Operator** oder **Feldwert** und klicken Sie auf die Schaltfläche **Ersetzen**.

3. Nachdem Sie alle Filter hinzugefügt haben, klicken Sie auf die Schaltfläche **Übernehmen**.

*Um noch einmal alle Objekte in der Liste der Quarantäne-Objekte anzuzeigen, öffnen Sie in der Konsolenstruktur das Kontextmenü für den Knoten **Quarantäne** und gehen Sie auf den Eintrag **Filter entfernen**.*

11.3. Untersuchung von Quarantäne-Objekten. Parameter der Aufgabe *Untersuchung von Quarantäne-Objekten*

Standardmäßig führt Anti-Virus nach jedem Update der Datenbanken die Systemaufgabe **Untersuchung von Quarantäne-Objekten** aus. Die Aufgabenparameter stehen in der Tabelle 8. Die Werte lassen sich nicht ändern.

Sie können den Zeitplan für die Aufgabe **Untersuchung von Quarantäne-Objekten** ändern oder sie von Hand starten.

Wenn die Quarantäne-Objekte nach dem Update der Datenbanken untersucht worden sind, kann Anti-Virus einige Objekte in der Quarantäne als nicht infiziert einstufen: Der Status dieser Objekte ändert sich in der Liste in **Bearbeitungsfehler**. Anti-Virus kann andere Objekte als infiziert einstufen und für sie Aktionen ausführen, die in den Parametern für die Aufgabe zur Virensuche **Untersuchung von Quarantäne-Objekten** vorgegeben sind: **Desinfizieren, irreparable Objekte löschen**.

Tabelle 8. Parameter der Aufgabe **Untersuchung von Quarantäne-Objekten**

Parameter der Aufgabe Quarantäne-Untersuchung	Wert
Untersuchungsbereich	Quarantäne-Ordner
Parameter für Sicherheit	Einheitlich für den gesamten Untersuchungsbereich, Werte stehen in der Tabelle 9.

Tabelle 9. Parameter für Sicherheit in der Aufgabe **Untersuchung von Quarantäne-Objekten**

Sicherheitsparameter	Wert
Zu untersuchende Objekte (s. Pkt. B.3.2 auf S. 397)	Alle Objekte
Nur neue und veränderte Objekte untersuchen (s. Pkt. B.3.3 auf S. 399)	Deaktiviert
Aktionen für infizierte Objekte (s. Pkt. B.3.5 auf S. 401)	Desinfizieren, löschen, wenn Desinfizieren nicht möglich ist
Aktion für verdächtige Objekte (s. Pkt. B.3.6 auf S. 403)	Überspringen
Objekte ausschließen (s. Pkt. B.3.8 auf S. 407)	Nein
Bedrohungen ausschließen (s. Pkt. B.3.9 auf S. 408)	Nein
Maximale Dauer der Objekt-Untersuchung (s. Pkt. B.3.10 auf S. 409)	Nicht vorgegeben

Sicherheitsparameter	Wert
Maximale Größe des zu untersuchenden Objektes (s. Pkt. B.3.11 auf S. 410)	Nicht vorgegeben
Zusätzliche Ströme des Dateisystems untersuchen (NTFS) (s. Pkt. B.3.2 auf S. 397)	Eingeschaltet
Bootsektoren untersuchen (s. Pkt. B.3.2 auf S. 397)	Deaktiviert
Technologie iChecker verwenden (s. Pkt. B.3.12 auf S. 410)	Ausgeschaltet
Technologie iSwift verwenden (s. Pkt. B.3.13 auf S. 411)	Ausgeschaltet
Compound-Objekte untersuchen (s. Pkt. B.3.4 auf S. 400)	• Archive* • SFX-Archive* • Gepackte Objekte* • eingebettete OLE-Objekte* * Der Parameter **Nur neue und veränderte Objekte** ist deaktiviert.

11.4. Objekte aus Quarantäne wiederherstellen

Anti-Virus verschiebt verdächtige Objekte verschlüsselt in den Quarantäne-Ordner, damit der geschützte Server vor schädlichen Wirkungen bewahrt wird.

Sie können jedes Objekt aus der Quarantäne wiederherstellen. Das kann in folgenden Fällen notwendig sein:

- Wenn nach der Quarantäne-Untersuchung anhand der aktualisierten Datenbanken der Status des Objektes in **Bearbeitungsfehler** oder **Desinfiziert** geändert worden ist.
- wenn Sie das Objekt für den Server als nicht gefährlich einschätzen und es benutzen wollen. Damit Anti-Virus dieses Objekt bei künftigen Untersuchungen nicht isoliert, können Sie das Objekt von der Untersuchung in der Aufgabe **Echtzeitschutz für Dateien** und in die Aufgabe zur Vi-

rensuche ausschließen. Geben Sie dazu das Objekt als Wert für den Parameter für Sicherheit unter **Ausschluss von Objekten** (nach Dateiname) (s. B.3.8 auf S. 407) oder **Ausschluss von Bedrohungen** (s. Pkt. B.3.9 auf S. 408) in diesen Aufgaben an.

Beim Wiederherstellen eines Objektes können Sie entscheiden, wo das wiederhergestellte Objekt gespeichert werden soll: An den ursprünglichen Speicherplatz (Standardeinstellung), in einen bestimmten Ordner für wiederhergestellte Objekte auf dem geschützten Server oder in einen von Ihnen angegebenen Ordner auf dem Rechner, auf dem die Anti-Virus-Konsole installiert ist, oder auf einem anderen Computer im Netzwerk.

Der *Ordner für Wiederherstellung* ist zum Speichern von wiederhergestellten Objekten auf dem geschützten Server vorgesehen. Sie können für dessen Untersuchung bestimmten Parameter für Sicherheit aktivieren. Der Pfad zu diesem Ordner wird mit den Quarantäne-Parametern eingegeben (s. Pkt. 11.8 auf S. 185).

Achtung!

Die Wiederherstellung von Objekten aus der Quarantäne kann den Computer infizieren.

Anmerkung

Wenn ein in die Quarantäne verschobenes Objekt zu einem Compound-Objekt gehört (z. B., ein Archive), fügt Anti-Virus es nicht wieder in dieses Compound-Objekt ein, sondern speichert es separat in einem ausgewählten Ordner.

Sie können ein Objekt wiederherstellen, nachdem dessen Kopie im Quarantäne-Ordner gespeichert worden ist, damit Sie es weiter benutzen können, beispielsweise, um das Objekt nach einem Update der Datenbanken noch einmal zu untersuchen.

Sie können ein Objekt oder mehrere Objekte wiederherstellen.

Um Objekte aus der Quarantäne wiederherzustellen, machen Sie Folgendes:

1. Gehen Sie in der Konsolenstruktur auf den Knoten **Quarantäne**.
2. Im Ergebnisfenster führen Sie eine der folgenden Aktionen aus:
   - Um ein Objekt wiederherzustellen, öffnen Sie das Kontextmenü mit einem Rechtsklick auf das Objekt, das Sie wiederherstellen wollen, und gehen Sie auf **Wiederherstellen**.
   - Um mehrere Objekte wiederherzustellen, markieren Sie die gewünschten Objekte mit der Taste **<Ctrl>** bzw. **<Shift>**, danach öffnen Sie mit einem Rechtsklick auf eines der markierten Objekte und gehen auf **Wiederherstellen**.

Es öffnet sich das Dialogfenster **Objektwiederherstellung** (s. Abbildung 66).

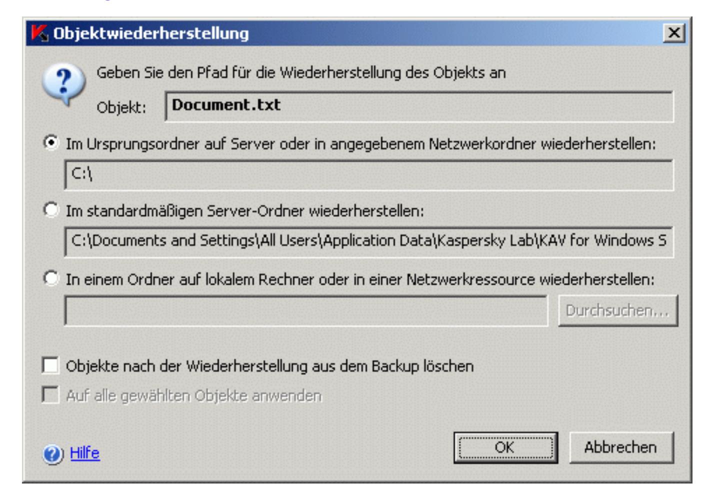


Abbildung 66. Dialogfenster **Objektwiederherstellung**

3. Im Dialogfenster **Objektwiederherstellung** geben Sie für jedes markierte Objekt den Ordner an, in den das wiederhergestellte Objekt (Objektname wird im Feld **Objekt** im oberen Teil des Dialogfensters angezeigt; bei mehreren Objekten wird der Name des ersten Objektes in der Markierungsliste angezeigt) gespeichert werden soll.

   Führen Sie eine der Aktionen durch:

   - um ein Objekt am ursprünglichen Speicherplatz wiederherzustellen, gehen Sie auf **Im Ursprungsordner auf Server oder in angegebenem Netzwerkordner wiederherstellen**.
   - um ein Objekt in einem Ordner wiederherzustellen, den Sie als Ordner für wiederhergestellte Objekte in den Quarantäne-Parametern angegeben haben (s. Pkt. B.6.4 auf S. 432), gehen Sie auf **Im standardmäßigen Server-Ordner wiederherstellen**.
   - um ein Objekt in einem anderen Ordner auf dem Computer zu speichern, auf dem die Anti-Virus-Konsole installiert ist, oder in einem Netzwerkordner, gehen Sie auf **In einem Ordner auf lokalem Rechner oder in einer Netzwerkressource wiederherstellen**, und danach wählen Sie den gewünschten Ordner aus oder Sie geben dessen Pfad ein.

4. Wenn Sie nach der Wiederherstellung eine Kopie vom Objekt im Quarantäne-Ordner speichern wollen, entfernen Sie das Häkchen im Kont-

rollkästchen **Objekte nach der Wiederherstellung aus dem Backup löschen**.

5. Um die eingegebenen Bedingungen für das Wiederherstellen auf die übrigen ausgewählten Objekte anzuwenden, setzen Sie das Häkchen im Kontrollkästchen **Auf alle gewählten Objekte anwenden**.

   Jedes ausgewählte Objekt wird an dem von Ihnen eingegebenen Speicherort wiederhergestellt und gespeichert: Wenn Sie **Im standardmäßigen Server-Ordner wiederherstellen** angegeben haben, wird jedes Objekt an seinem ursprünglichen Speicherplatz wiederhergestellt; wenn Sie **Im standardmäßigen Server-Ordner wiederherstellen** oder **In einem Ordner auf lokalem Rechner oder in einer Netzwerkressource wiederherstellen** angegeben haben, werden alle Objekte in diesem einen angegebenen Ordner gespeichert.

6. Klicken Sie auf die Schaltfläche **OK**.

   Anti-Virus beginnt damit, das erste von Ihnen ausgewählte Objekt wiederherzustellen.

7. Wenn das Objekt mit diesem Namen am angegebenen Speicherort bereits vorhanden ist, öffnet sich das Dialogfenster **Objekt mit diesem Namen ist bereits vorhanden** (s. Abbildung 67).

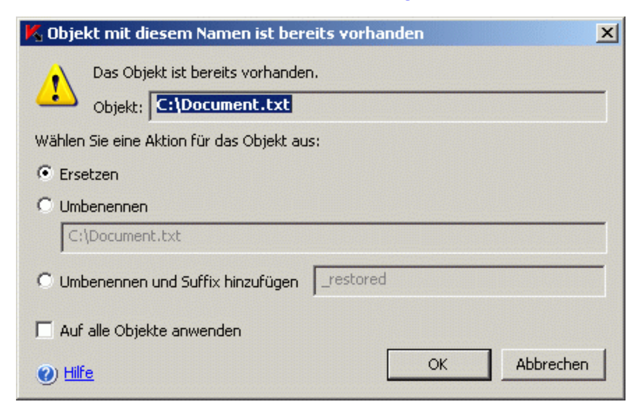


Abbildung 67. Dialogfenster **Objekt mit diesem Namen ist bereits vorhanden**

a) Wählen Sie eine der folgenden Anti-Virus-Aktionen:

   - **Ersetzen**, um das wiederhergestellte Objekt anstelle des vorhandenen Objektes zu speichern
   - **Umbenennen**, um das wiederhergestellte Objekt unter einem anderen Namen zu speichern. Im Eingabefeld tragen Sie einen

neuen Dateinamen für das Objekt und den vollständigen Pfad ein.

- **Umbenennen und Suffix hinzufügen**, um das Objekt umzubenennen und der Datei einen Suffix hinzuzufügen. Tragen Sie das Suffix in das Eingabefeld ein.

b) Wenn Sie mehrere Objekte für die Wiederherstellung ausgewählt haben, setzen Sie, damit die ausgewählte Aktion **Ersetzen** oder **Umbenennen und Suffix hinzufügen** für die übrigen ausgewählten Objekte angewendet werden kann, das Häkchen im Kontrollkästchen **Auf alle Objekte anwenden**.

(Wenn Sie **Umbenennen** angegeben haben, kann das Häkchen im Kontrollkästchen **Auf alle Objekte anwenden** nicht gesetzt werden.)

c) Klicken Sie auf die Schaltfläche **OK**.

Das Objekt wird wiederhergestellt. Die Daten zum Wiederherstellungsvorgang werden im Bericht zum System-Audit registriert.

Wenn Sie nicht die Variante **Auf alle Objekte anwenden** im Dialogfenster **Objektwiederherstellung** ausgewählt haben, öffnet sich das Dialogfenster **Objektwiederherstellung** noch einmal. Sie können dort den Speicherort angeben, an dem das folgende ausgewählte Objekt wiederhergestellt werden soll (s. Schritt 3 dieses Verfahrens).

11.5. Dateien in Quarantäne verschieben

Sie können manuell Dateien in die Quarantäne verschieben.

Um Dateien in die Quarantäne zu verschieben, machen Sie Folgendes:

1. In der Konsolenstruktur öffnen Sie das Kontextmenü für den Knoten **Quarantäne** und gehen Sie auf den Eintrag **Hinzufügen**.
2. Im Dialogfenster **Datei öffnen** wählen Sie die Dateien auf dem Datenträger aus, die Sie in die Quarantäne verschieben wollen, und klicken auf die Schaltfläche **OK**.

Anmerkung

Wenn Dateien, die Sie in die Quarantäne verschieben wollen, in einem einzigen Ordner gespeichert sind, können Sie im Dialogfenster **Datei öffnen** mehrere Dateien markieren, indem Sie die Taste **<Ctrl>** bzw. **<Shift>** festhalten.

Anti-Virus verschiebt die ausgewählte Datei (ausgewählten Dateien) in die Quarantäne.

3. Im Dialogfenster mit dem Namen der ersten markierten Datei führen Sie die folgende Aktion aus (wenn Sie die Aktion für alle markierten Dateien ausführen wollen, setzen Sie das Häkchen in **Auf alle Objekte anwenden**:

   - Um die Datei im Ursprungsordner zu speichern, klicken Sie auf die Schaltfläche **Speichern**.

   - Um die Datei im Ursprungsordner zu löschen, klicken Sie auf die Schaltfläche **Löschen**.

11.6. Objekte aus Quarantäne löschen

Gemäß den Parametern der Aufgabe **Untersuchung von Quarantäne-Objekten** (s. Pkt. 11.3 auf S. 175) löscht Anti-Virus automatisch aus dem Quarantäne-Ordner diejenigen Objekte, deren Status sich bei der Quarantäne-Untersuchung anhand aktualisierter Datenbanken in **Infiziert** geändert hat und die Anti-Virus nicht reparieren konnte. Die übrigen Objekte löscht Anti-Virus nicht aus der Quarantäne.

Sie können ein Objekt oder mehrere Objekte manuell aus der Quarantäne löschen.

Um ein Objekt oder mehrere Objekte aus der Quarantäne zu löschen, machen Sie Folgendes:

1. Gehen Sie in der Konsolenstruktur auf den Knoten **Quarantäne**.

2. Führen Sie eine der Aktionen durch:

   - Um ein Objekt zu löschen, öffnen Sie das Kontextmenü mit einem Rechtsklick auf das Objekt, das Sie löschen wollen, und gehen Sie auf **Löschen**.

   - Um mehrere Objekte zu löschen, markieren Sie die gewünschten Objekte mit der Taste **<Ctrl>** bzw. **<Shift>**, danach öffnen Sie das

Kontextmenü mit einem Rechtsklick auf eines der markierten Objekte und gehen auf **Löschen**.

3. Im Dialogfenster **Bestätigung** klicken Sie auf die Schaltfläche **Ja**, um den Vorgang zu bestätigen.

11.7. Verdächtige Quarantäne-Objekte zur Analyse in das Virenlabor einschicken

Wenn das Verhalten einer Datei den Verdacht nahe legt, dass in ihr eine Bedrohung vorhanden ist, Anti-Virus diese Datei aber als nicht infiziert einstuft, dann haben Sie möglicherweise eine neue, unbekannte Bedrohung angetroffen, deren Reparaturalgorithmus noch nicht in den Datenbanken steht. Sie können diese Datei zur Analyse in das Virenlabor von Kaspersky Lab einschicken. Die Viren-Analytiker von Kaspersky Lab untersuchen die Datei, und wenn sie darin eine neue Bedrohung entdecken, erstellen sie einen identifizierenden Eintrag und Reparaturalgorithmen in den Datenbanken. So kann es sein, dass, wenn Sie das Objekt nach einem Update der Datenbanken noch einmal untersuchen, Anti-Virus die Datei als infiziert einstuft und er sie reparieren kann. Auf diese Weise retten Sie nicht nur das Objekt, sondern verhindern auch noch eine Virenepidemie.

Sie können nur Dateien aus der Quarantäne zur Analyse einsenden. Im Quarantäne-Ordner werden sie in verschlüsselter Form gespeichert und werden von der Antiviren-Anwendung, die auf dem Mail-Server installiert ist, beim Verschicken nicht gelöscht.

Sie können eine Datei aus der Quarantäne zur Analyse einschicken, der Anti-Virus den Status *Verdächtig* oder *Warnung* zugewiesen hat. Sie können keine Datei aus der Quarantäne zur Analyse einschicken, der Anti-Virus den Status *Infiziert* zugewiesen hat. Details dazu, wie Anti-Virus Bedrohungen in Objekten erkennt, finden Sie in Pkt. 1.1.3 auf S. 19.

Anmerkung

Sie können keine Objekte in die "Kaspersky Lab" zur Untersuchung schicken, nach dem Ablauf des Schlüssels.

Um eine verdächtige Datei zur Analyse in Virenlabor einzuschicken, machen Sie Folgendes:

1. Wenn sich die Datei nicht in der Quarantäne befindet, verschieben Sie sie zuerst in die Quarantäne (s. Pkt. 11.5 auf S. 181).

2. Im Knoten **Quarantäne** öffnen Sie in der Liste mit den Quarantäne-Objekten das Kontextmenü durch Rechtsklick auf die Datei, die Sie zur Analyse einschicken wollen, und gehen Sie auf **Zu Kaspersky Lab schicken**.

3. Wenn auf dem Rechner, auf dem die Anti-Virus-Konsole installiert ist, ein Mail-Client eingerichtet ist, wird eine neue E-Mail-Nachricht erstellt. Schauen Sie sich die Nachricht an und klicken Sie danach auf die Schaltfläche **Einschicken**.

   Das Feld **Empfänger** enthält die E-Mail-Adresse des Virenlabors mailto:newvirus@kaspersky.com. Im Feld **Betreff** steht der Text "Quarantäne-Objekt".

   Der Nachrichtenkörper enthält den Text "Objekt wird zur Analyse an Kaspersky Lab geschickt". Sie können dem Nachrichtenkörper beliebige Zusatzinformationen über die Datei hinzufügen, z.B. warum Sie die Datei für verdächtig halten, wie sie sich verhält und wie sie das System beeinflusst.

   An die Nachricht wird das Archiv *<Objektname>.cab* angehängt. Es enthält die Datei *<uuid>.klq* mit dem verschlüsselten Objekt, die Datei *<uuid>.txt* mit Daten, die Anti-Virus über das Objekt zusammengetragen hat, sowie die Datei *Sysinfo.txt*, die die folgenden Informationen über den Anti-Virus und das Betriebssystem des Servers enthält:

   - Name und Version des Betriebssystems
   - Name und Version des Anti-Virus
   - Erstellungsdatum des zuletzt installierten Datenbank-Updates
   - Seriennummer des aktiven Lizenzschlüssels

   Die angegebenen Informationen brauchen die Virenanalytiker von Kaspersky Lab, um die Datei schneller und effektiver zu bearbeiten. Wenn Sie diese Daten jedoch nicht übertragen wollen, können Sie die Datei *Sysinfo.txt* aus dem Archiv löschen.

4. Wenn auf dem Rechner, auf dem die Anti-Virus-Konsole installiert ist, kein Mail-Client eingerichtet ist, öffnet sich das Fenster des Verbindungsassistenten von Microsoft für die Herstellung einer Internetverbindung. Sie können folgende Aktionen vornehmen:

   - Wenn Sie den Anweisungen des Assistenten für die Herstellung einer Internetverbindung folgen, erstellen Sie ein neues Benutzerkonto und schicken die Datei von diesem Rechner los.
   - Sie verlassen den Assistenten und speichern das markierte verschlüsselte Objekt in eine Datei. Die Datei können Sie selbstständig zur Analyse in das Virenlabor einschicken.

Um ein verschlüsseltes Objekt in einer Datei zu speichern, machen Sie Folgendes:

a) Im Dialogfenster für die Speicherung des Objektes (s. Abbildung 68) klicken Sie auf die Schaltfläche **OK**.

b) Markieren Sie den Ordner auf dem Datenträger des geschützten Servers oder den Netzwerkordner, in den Sie die Datei mit dem Objekt speichern wollen.

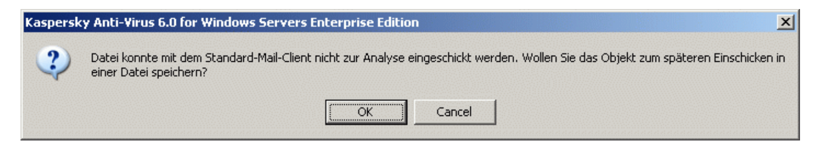


Abbildung 68. Dialogfenster mit Aufforderung zum Speichern des Quarantäne-Objektes in einer Datei

11.8. Quarantäne-Parameter einstellen

In diesem Abschnitt werden die Einstellungen der Quarantäne-Parameter beschrieben. Die neuen Parameterwerte der Quarantäne werden sofort nach dem Speichern übernommen.

Die Beschreibung der Quarantäne-Parameter und deren Standardwerte finden Sie in Pkt. B.6 auf S. 430.

Um die Quarantäne-Parameter einzustellen, machen Sie Folgendes:

1. In der Konsolenstruktur öffnen Sie das Kontextmenü für den Knoten **Quarantäne** und gehen Sie auf den Eintrag **Eigenschaften** (s. Abbildung 69).

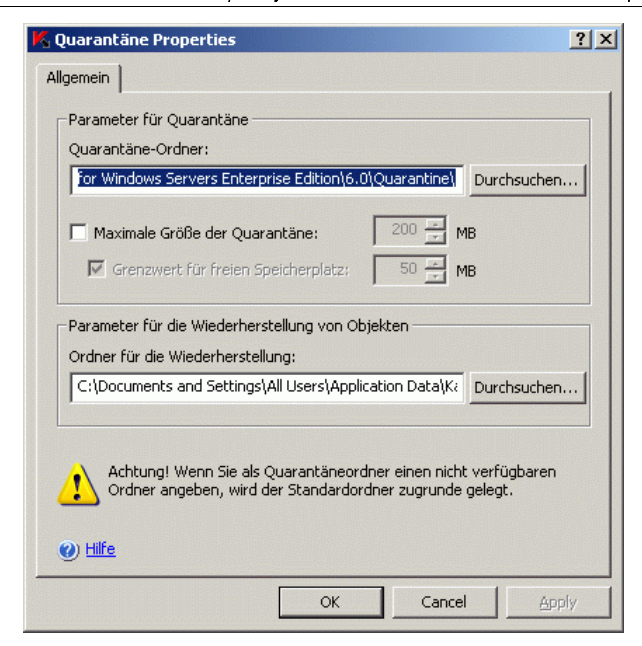


Abbildung 69. Dialogfenster **Eigenschaften: Quarantäne**

2. Im Dialogfenster **Eigenschaften: Quarantäne** konfigurieren Sie die gewünschten Quarantäne-Parameter je nach Ihren Wünschen:

   - Um einen Quarantäne-Ordner anzugeben, der vom Standardordner abweicht, markieren Sie im Feld **Quarantäne-Ordner** den gewünschten Ordner auf dem lokalen Datenträger des geschützten Servers oder geben Sie dessen Namen und Pfad an (Details zum Parameter finden Sie in Pkt. B.6.1 auf S. 430).

   - Um die maximale Größe der Quarantäne festzulegen, setzen Sie das Häkchen in **Maximale Größe der Quarantäne** und tragen Sie im Eingabefeld den gewünschten Parameterwert in Megabyte ein (s. Pkt. B.6.2 auf S. 431).

   - Um die minimale Größe des freien Speicherplatzes in der Quarantäne festzulegen, wählen Sie den Parameter **Maximale Größe der Quarantäne**, aktivieren Sie das Kontrollkästchen **Grenzwert für freien Speicherplatz** und tragen Sie im Eingabefeld den gewünschten Parameterwert in Megabyte ein (s. Pkt. B.6.3 auf S. 432).

   - Um einen anderen Wiederherstellungsordner anzugeben, wählen Sie in der Parametergruppe **Parameter für die Wiederherstellung**

von Objekten den gewünschten Ordner auf dem lokalen Datenträger des geschützten Servers oder geben sie den Namen und vollständigen Pfad ein. (s. Pkt. B.6.4 auf S. 432).

3. Klicken Sie auf die Schaltfläche **OK**.

11.9. Statistik für Quarantäne

Sie können Informationen über die Menge an Objekten in der Quarantäne einsehen, die so genannte *Statistik für Quarantäne*.

Um die Statistik für Quarantäne anzuzeigen, öffnen Sie das Kontextmenü für den Knoten ***Quarantäne*** *in der Konsolenstruktur und gehen Sie auf den Eintrag* ***Statistik anzeigen*** *(s. Abbildung 70).*

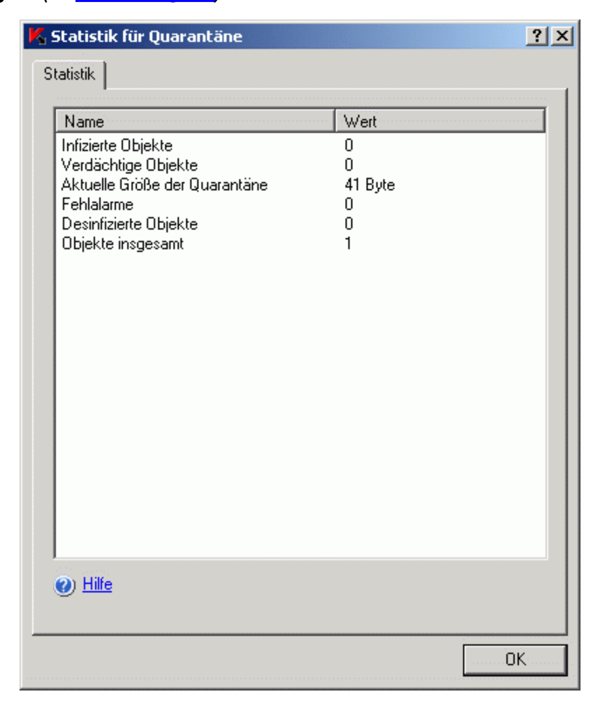


Abbildung 70. Dialogfenster **Statistik für Quarantäne**

Im Dialogfenster **Statistik für Quarantäne** werden die folgenden Informationen über die derzeitige Menge an Objekten in der Quarantäne dargestellt:

Feld	Beschreibung
Infizierte Objekte	Menge der infizierten Objekte: a) die nach der Quarantäne-Untersuchung den Status *Infiziert* zugewiesen bekommen haben, und die Anti-Virus nicht desinfizieren oder löschen konnte, und b) die Anti-Virus gemäß den Parameterwert **Aktion für Objekte je nach Bedrohungstyp** in die Quarantäne verschoben hat.
Verdächtige Objekte	Menge an verdächtigen Objekten und potentiell gefährlichen Objekten. Details dazu, wie Anti-Virus Bedrohungen in Objekten erkennt, finden Sie in Pkt. 1.1.3 auf S. 19.
Aktuelle Größe der Quarantäne	Summe der Daten im Quarantäne-Ordner
Fehlalarme	Menge an Objekten, die den Status **Falsche Verarbeitung** zugewiesen bekommen haben, weil sie bei der Quarantäne-Untersuchung anhand der aktualisierten Datenbanken als nicht infiziert eingestuft werden mussten.
Desinfizierte Objekte	Menge an Objekten, die nach der Quarantäne-Untersuchung den Status **Desinfiziert** zugewiesen bekommen haben
Objekte insgesamt	Summe der Objekte in der Quarantäne

KAPITEL 12. SICHERUNGSKOPIEREN VON OBJEKTEN VOR DESINFEKTION / LÖSCHEN. ISOLIEREN IM BACKUP

In diesem Kapitel stehen die folgenden Informationen:

- Sicherungskopieren von Objekten vor deren Desinfektion / Löschen (s. 12.1 auf S. 189)
- Dateien im Backup anzeigen, sortieren und filtern (s. Pkt. 12.2 auf S. 190)
- Dateien aus Backup wiederherstellen (s. Pkt. 12.3 auf S. 195)
- Dateien aus Backup löschen (s. Pkt. 12.4 auf S. 199)
- Einstellung der Backup-Parameter (s. Pkt. 12.5 auf S. 199)
- Statistik für Backup (s. Pkt. 12.6 auf S. 201)

Parameter von Backup sind in Pkt. B.7 auf S. 433 beschrieben.

12.1. Sicherungskopieren von Objekten vor Desinfektion / Löschen

Bevor eine infizierte Datei desinfiziert oder gelöscht wird, die den Status **Infiziert** hat, speichert Anti-Virus deren verschlüsselte Kopie in einem besonderen Ordner, im *Backup*.

Anti-Virus verschiebt außerdem in den Backup verschlüsselte Kopien der Dateien mit dem Status **Verdächtig** oder **Potentiell gefährlich**, wenn Sie in den Parametern für Sicherheit der Aufgabe **Echtzeitschutz für Dateien** oder der Aufgaben zur Virensuche als Aktion für verdächtige Objekte **Löschen** ausgewählt haben.

Wenn das Objekt zu einem Compound-Objekt gehört (z. B., Archiv), wird im Backup die Datei mit dem kompletten Compound-Objekt gespeichert.

Sie können Dateien aus dem Backup wiederherstellen, im ursprünglichen Ordner oder in einem anderen Ordner auf dem geschützten Server oder auf einem anderen Rechner im lokalen Netzwerk. Sie können eine Datei aus dem Backup wiederherstellen, beispielsweise, wenn die ursprüngliche infizierte Datei wichtige Informationen enthält, bei der Reparatur dieser Datei Anti-Virus deren Integrität nicht retten konnte und aufgrund dessen auf die Informationen nicht mehr zugegriffen werden kann.

Achtung!

Die Wiederherstellung von Dateien aus dem Backup kann den Computer infizieren.

12.2. Dateien im Backup sortieren

Sie können Dateien im Backup-Ordner lediglich in der Anti-Virus-Konsole im Knoten **Backup** anzeigen lassen. Sie können die Dateien mit den Datei-Managern von Microsoft Windows nicht betrachten.

Um Dateien im Backup anzuzeigen, gehen Sie in der Konsolenstruktur auf den Knoten ***Backup*** *(s. Abbildung 71).*

Um ein gewünschtes Objekt in der Liste zu suchen, können Sie die Objekte sortieren (s. Pkt. 12.2.1 auf S. 193) oder filtern (s. Pkt. 12.2.2 auf S. 193).

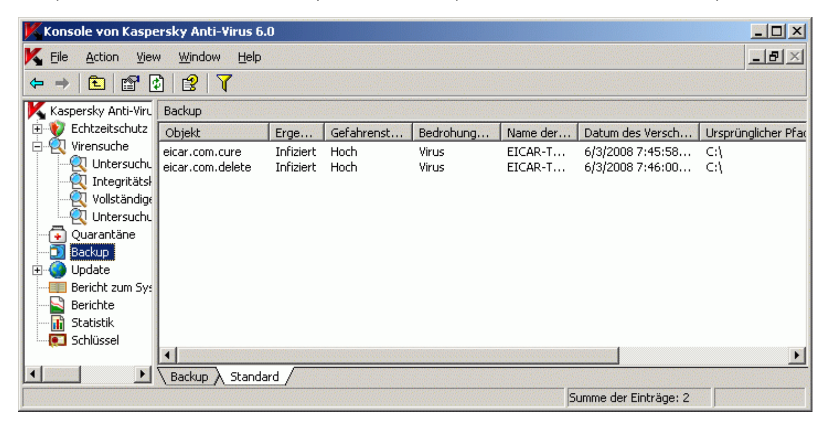


Abbildung 71. Informationen über Dateien im Backup in der Anti-Virus-Konsole

Im Ergebnisfenster werden die folgenden Informationen zu einer Datei im Backup angezeigt:

Feld	Beschreibung
Objekt	Name der Datei, deren Kopie im Backup gespeichert ist
Ergebnis	Status der Datei, ob in ihr Bedrohungen vorhanden sind oder nicht: • **Infiziert**. Es wurde eine komplette Übereinstimmung von Codebestandteilen der Datei mit Codebestandteilen von einer bekannten Bedrohung festgestellt. • **Verdächtig**. Es wurde eine partielle Übereinstimmung von Codebestandteilen der Datei mit Codebestandteilen von einer bekannten Bedrohung festgestellt. • **Potentiell gefährlich**. Die Datei hat Anti-Virus mit der heuristischen Analysemethode als potentiell gefährlich eingestuft. Details dazu, wie Anti-Virus Bedrohungen in Objekten erkennt, finden Sie in Pkt. 1.1.3 auf S. 19.
Gefahrenstufe	Die Gefahrenstufe zeigt an, wie gefährlich das Objekt für den Server ist. Die Gefahrenstufe hängt vom Bedrohungstyp im Objekt ab und kann die folgenden Werte annehmen: • **Hoch**. Die Datei könnte eine Bedrohung der Art *Netzwerkwürmer*, *klassische Viren*, *Trojanische Programme* oder eine Bedrohung eines nicht bestimmbaren Typs (zu diesem Typ gehören neue Viren, die zurzeit noch nicht einem bekannten Typ zugeordnet werden können) enthalten. • **Mittel**. Die Datei könnte eine Bedrohung des Typs *diverse schädliche Programme*, *Adware* oder *Pornware* enthalten. • **Niedrig**. Die Datei könnte eine Bedrohung des Typs *potentiell gefährliche Programme* enthalten. Details über die Bedrohungen, die Anti-Virus erkennen kann, finden Sie in Pkt. 1.1.2 auf S. 15.

Feld	Beschreibung
Bedrohungstyp	Die Bedrohungsart nach der Klassifizierung von Kaspersky Lab gehört zur vollständigen Bezeichnung einer Bedrohung, die Anti-Virus meldet, nachdem er eine Datei als infiziert oder verdächtig eingestuft hat. Sie können die vollständige Bezeichnung einer Bedrohung in einem Objekt im Knoten **Berichte** im Detailbericht über die Aufgabenausführung anzeigen.
Name der Bedrohung	Der Name der Bedrohung nach der Klassifizierung von Kaspersky Lab gehört zur vollständigen Bezeichnung einer Bedrohung, die Anti-Virus meldet, nachdem er eine Datei als infiziert eingestuft hat. Sie können die vollständige Bezeichnung einer Bedrohung in einem Objekt im Knoten **Berichte** im Detailbericht über die Aufgabenausführung anzeigen.
Datum des Verschiebens	Datum und Uhrzeit des Speichervorgangs für die Datei im Ordner des Backups
Ursprünglicher Pfad	Vollständiger Pfad zum Ausgangsordner, dem Ordner, im dem sich die Datei befand, bevor Anti-Virus deren Kopie im Backup gespeichert hat
Größe	Dateigröße
Benutzername	Die Spalte enthält folgende Daten: • Wenn die Datei von Anti-Virus in der Aufgabe **Echtzeitschutz für Dateien** in das Backup verschoben wurde – der Name des Benutzerkontos, mit dessen Rechten die Anwendung auf die Datei zugegriffen hat, als sie abgefangen wurde. • Wenn die Datei von Anti-Virus in einer Aufgabe zur Virensuche in das Backup verschoben wurde – der Name des Benutzerkontos, mit dessen Rechten die Aufgabe ausgeführt wurde.

Wie die Parameter des Backups eingestellt werden, finden Sie in Pkt. 12.5 auf S. 199.

12.2.1. Dateien im Backup sortieren

Standardmäßig werden die Dateien im Backup nach ihrem Speicherdatum in umgekehrter chronologischer Reihenfolge sortiert. Um die gewünschte Datei zu finden, können Sie die Dateien nach dem Spalteninhalt im Ergebnisfenster sortieren lassen.

Das Sortierergebnis wird gespeichert, wenn Sie den Knoten **Backup** verlassen oder wenn Sie die Anti-Virus-Konsole mit Speichern in der *msc*-Datei schließen und sie wieder aus dieser Datei wieder öffnen.

Um Dateien im Backup zu sortieren, machen Sie Folgendes:

1. Gehen Sie in der Konsolenstruktur auf den Knoten **Backup**.
2. In der Dateiliste des Backups klicken Sie auf den Spaltenkopf, nach dessen Inhalt Sie die Objekte sortieren wollen.

12.2.2. Dateien im Backup filtern

Um eine gewünschte Datei im Backup zu suchen, können Sie die Dateien *filtern*, also nur die Dateien im Knoten **Backup** anzeigen, die den von Ihnen eingegebenen Filterkriterien (Filtern) entsprechen.

Das Filterergebnis wird gespeichert, wenn Sie den Knoten **Backup** verlassen oder wenn Sie die Anti-Virus-Konsole mit Speichern in der *msc*-Datei schließen und sie wieder aus dieser Datei wieder öffnen.

Um Dateien im Backup zu filtern, machen Sie Folgendes:

1. In der Konsolenstruktur öffnen Sie das Kontextmenü für den Knoten **Backup** und gehen Sie auf den Eintrag **Filter**.

   Es öffnet sich das Dialogfenster **Filterparameter** (s. Abbildung 72).

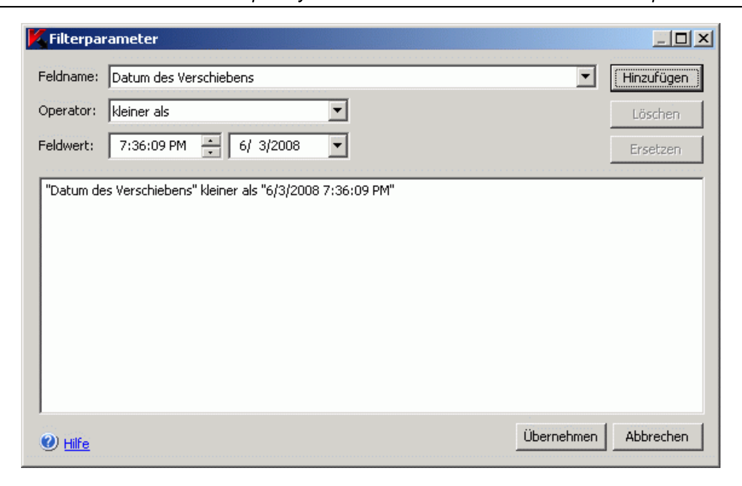


Abbildung 72. Dialogfenster **Filterparameter**

2. Um einen Filter hinzufügen, führen Sie folgende Aktionen durch:

   a) In der Liste **Feldname** wählen Sie ein Feld aus, mit dem der von Ihnen eingegebene Filterwert beim Selektieren verglichen wird.

   b) In der Liste **Operator** wählen Sie die Filterbedingung aus. Die Bedingungswerte für das Filtern in der Liste können sich voneinander unterscheiden, je nach dem, welchen Wert Sie im Feld **Feldname** ausgewählt haben.

   c) Im Feld **Feldwert** geben einen Filterwert ein oder markieren einen Filterwert.

   d) Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der hinzugefügte Filter wird in der Filterliste im Fenster **Filterparameter** dargestellt. Wiederholen Sie diese Vorgänge für jeden Filter, den Sie hinzufügen wollen. Wenn Sie mehrere Filter eingeben, werden sie mit einem logischen UND verknüpft.

- Um einen Filter zu löschen, markieren Sie den zu entfernenden Filter in der Filterliste und klicken Sie auf die Schaltfläche **Löschen**.

- Um einen Filter zu bearbeiten, markieren Sie ihn in der Filterliste des Dialogfensters **Filterparameter**, ändern Sie die gewünschten Werte in den Feldern **Feldname**, **Operator** oder **Feldwert** und klicken Sie auf die Schaltfläche **Ersetzen**.

3. Nachdem Sie alle Filter hinzugefügt haben, klicken Sie auf die Schaltfläche **Übernehmen**. In der Liste werden nur die Dateien dargestellt, die den von Ihnen eingegebenen Filtern entsprechen.

*Um noch einmal alle Dateien in der Liste der Backup-Dateien anzuzeigen, öffnen Sie in der Konsolenstruktur das Kontextmenü für den Knoten **Backup** und gehen Sie auf den Eintrag **Filter entfernen**.*

12.3. Dateien aus Backup wiederherstellen

Anti-Virus speichert Dateien im Backup im verschlüsselten Format, damit der geschützte Server vor schädlichen Wirkungen bewahrt wird.

Sie können Dateien aus dem Backup wiederherstellen.

In den folgenden Fällen müssen Sie möglicherweise eine Datei wiederherstellen:

- Wenn die Ursprungsdatei, die sich als infiziert herausgestellt hat, wichtige Informationen enthalten hat, bei der Reparatur dieser Datei Anti-Virus deren Integrität nicht retten konnte und aufgrund dessen auf die Informationen nicht mehr zugegriffen werden kann.
- wenn Sie die Datei für den Server als nicht gefährlich einschätzen und sie benutzen wollen. Damit Anti-Virus diese Datei bei künftigen Untersuchungen nicht als infiziert oder verdächtig einstuft, können Sie sie von der Untersuchung in der Aufgabe **Echtzeitschutz für Dateien** und in die Aufgabe zur Virensuche ausschließen. Geben Sie dazu die Datei als Parameter **Ausschluss von Objekten** (s. Pkt. B.3.8 auf S. 407) oder **Ausschluss von Bedrohungen** (s. Pkt. B.3.9 auf S. 408) an.

Achtung!

Die Wiederherstellung von Dateien aus dem Backup kann den Computer infizieren.

Beim Wiederherstellen einer Datei können Sie entscheiden, wo sie gespeichert werden soll: An den ursprünglichen Speicherplatz (Standardeinstellung), in einen bestimmten Ordner für wiederhergestellte Objekte auf dem geschützten Server oder in einen von Ihnen angegebenen Ordner auf dem Rechner, auf dem die Anti-Virus-Konsole installiert ist, oder auf einem anderen Computer im lokalen Netzwerk.

Der *Ordner für Wiederherstellung* ist zum Speichern von wiederhergestellten Objekten auf dem geschützten Server vorgesehen. Sie können für dessen Untersuchung bestimmten Parameter für Sicherheit aktivieren. Der Pfad zu diesem Ordner wird mit den Backup-Parametern eingegeben (s. Pkt. 12.5 auf S. 199).

Standardmäßig löscht Anti-Virus beim Wiederherstellen einer Datei deren Kopie aus dem Backup. Sie können die Kopie der Datei im Backup nach deren Wiederherstellung speichern.

Um Dateien aus dem Backup wiederherzustellen, machen Sie Folgendes:

1. Gehen Sie in der Konsolenstruktur auf den Knoten **Backup**.

2. Führen Sie eine der Aktionen durch:

   - um eine Datei wiederherzustellen, öffnen Sie das Kontextmenü in der Dateiliste des Backups mit einem Rechtsklick auf die Datei, die Sie wiederherstellen wollen, und gehen Sie auf **Wiederherstellen**.

   - Um mehrere Dateien wiederherzustellen, markieren Sie die gewünschten Dateien in der Liste mit der Taste **<Ctrl>** bzw. **<Shift>**, danach öffnen Sie das Kontextmenü mit einem Rechtsklick auf eine der markierten Dateien und gehen auf **Wiederherstellen**.

3. Im Dialogfenster **Objektwiederherstellung** (s. Abbildung 73) geben Sie den Ordner ein, in den die wiederhergestellte Datei gespeichert werden soll.

   Der Dateiname wird im Feld **Objekt** im oberen Teil des Dialogfensters angezeigt. Wenn Sie mehrere Dateien markiert haben, wird der Name der ersten Datei in der Auswahlliste angezeigt.

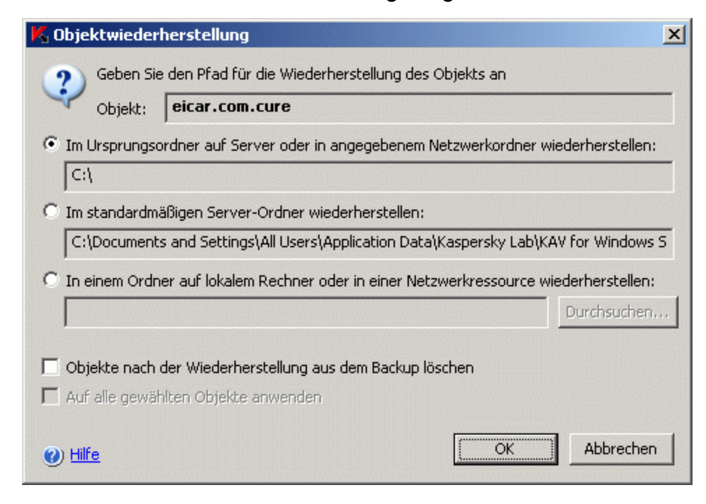


Abbildung 73. Dialogfenster **Objektwiederherstellung**

Führen Sie eine der Aktionen durch:

- um eine wiederhergestellte Datei auf dem geschützten Server zu speichern, gehen Sie auf:
  - **Ursprünglicher Ordner**, wenn Sie die Datei im Ausgangsordner wiederherstellen wollen, oder
  - **Standardordner für Wiederherstellung**, wenn Sie eine Datei in einem Ordner wiederherstellen wollen, den Sie als Ordner für wiederhergestellte Objekte in den Backup-Parametern Backup angegeben haben (s. Pkt. 12.5 auf S. 199)
- um eine wiederhergestellte Datei in einem anderen Ordner zu speichern, gehen Sie unter der Überschrift **Wiederherstellung mit Konsole** auf **In angegebenen Ordner speichern** und wählen Sie den gewünschten Ordner aus (auf dem Rechner, auf dem die Anti-Virus-Konsole installiert ist oder einen Netzwerkordner) oder Sie geben dessen Pfad ein.

4. Wenn Sie nach der Wiederherstellung eine Kopie von der Datei im Backup-Ordner speichern wollen, entfernen Sie das Häkchen im Kontrollkästchen **Objekte nach der Wiederherstellung aus dem Backup löschen**.

5. Wenn Sie mehrere Dateien für die Wiederherstellung ausgewählt haben, setzen Sie, damit die genannten Speicherbedingungen für die übrigen ausgewählten Dateien angewendet werden kann, das Häkchen im Kontrollkästchen **Auf alle gewählten Objekte anwenden**.

   Jede ausgewählte Datei wird in dem von Ihnen eingegebenen Ordner wiederhergestellt und gespeichert: Wenn Sie **Ursprünglicher Ordner** angegeben haben, wird jede Datei an ihrem ursprünglichen Speicherplatz wiederhergestellt; wenn Sie **Standardordner für wiederhergestellte Objekte** oder **Angegebener Ordner auf anderem Rechner** angegeben haben, werden alle Dateien in diesem einen angegebenen Ordner gespeichert.

6. Klicken Sie auf die Schaltfläche **OK**.

   Anti-Virus beginnt damit, die erste von Ihnen ausgewählte Datei wiederherzustellen.

7. Wenn die Datei mit diesem Namen im angegebenen Ordner bereits vorhanden ist, öffnet sich das Dialogfenster **Objekt mit diesem Namen ist bereits vorhanden** (s. Abbildung 74).

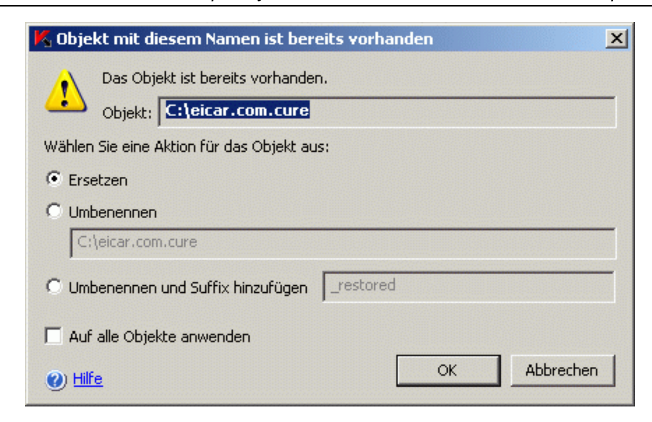


Abbildung 74. Dialogfenster **Objekt mit diesem Namen ist bereits vorhanden**

Führen Sie die folgenden Aktionen aus:

a) Wählen Sie eine Speicherbedingung für die wiederhergestellte Datei aus:

   - **Ersetzen**, um die wiederhergestellte Datei anstelle der vorhandenen Datei zu speichern
   - **Umbenennen**, um die wiederhergestellte Datei unter einem anderen Namen zu speichern. Im Eingabefeld tragen Sie einen neuen Dateinamen und den vollständigen Pfad ein.
   - **Umbenennen und Suffix hinzufügen**, um das Objekt umzubenennen und der Datei einen Suffix hinzuzufügen. Tragen Sie das Suffix in das Eingabefeld ein.

b) Wenn Sie die ausgewählte Aktion **Ersetzen** oder **Umbenennen und Suffix hinzufügen** für die übrigen ausgewählten Objekte anwenden wollen, setzen Sie das Häkchen im Kontrollkästchen **Auf alle Objekte anwenden**.

   (Wenn Sie **Umbenennen** angegeben haben, kann das Häkchen im Kontrollkästchen **Auf alle Objekte anwenden** nicht gesetzt werden.)

c) Klicken Sie auf die Schaltfläche **OK**.

   Die Datei wird wiederhergestellt. Die Daten zum Wiederherstellungsvorgang werden im Bericht zumSystem-Audit registriert.

   Wenn Sie mehrere Dateien zur Wiederherstellung markiert und nicht die Variante **Auf alle Objekte anwenden** im Dialogfenster **Objektwiederherstellung** ausgewählt haben, öffnet sich das Dia-

logfenster **Objektwiederherstellung** noch einmal. Sie können dort einen Ordner angeben, in dem beim Wiederherstellen die folgende ausgewählte Datei gespeichert werden soll (s. Schritt 3 dieses Verfahrens).

12.4. Dateien aus Backup löschen

Um eine oder mehrere Dateien aus dem Backup zu löschen, machen Sie Folgendes:

1. Gehen Sie in der Konsolenstruktur auf den Knoten **Backup**.
2. Führen Sie eine der Aktionen durch:
   - Um eine Datei zu löschen, öffnen Sie das Kontextmenü mit einem Rechtsklick auf die Datei, die Sie löschen wollen, und gehen Sie auf **Löschen**.
   - Um mehrere Dateien zu löschen, markieren Sie die gewünschten Dateien in der Liste mit der Taste **<Ctrl>** bzw. **<Shift>**, danach öffnen Sie das Kontextmenü mit einem Rechtsklick auf eine der markierten Dateien und gehen auf **Löschen**.
3. Im Dialogfenster **Bestätigung** klicken Sie auf die Schaltfläche **Ja**, um den Vorgang zu bestätigen. Die ausgewählten Dateien werden gelöscht.

12.5. Backup-Parameter einstellen

In diesem Abschnitt wird beschrieben, wie die Backup-Parameter eingestellt werden. Die Beschreibung der Backup-Parameter und dessen Standardwerte finden Sie in Pkt. B.7 auf S. 433.

Die neuen Parameterwerte des Backups werden sofort nach dem Speichern übernommen.

Um die Backup-Parameter einzustellen, machen Sie Folgendes:

1. In der Konsolenstruktur öffnen Sie das Kontextmenü für den Knoten **Backup** und gehen Sie auf den Eintrag **Eigenschaften** (s. Abbildung 75).

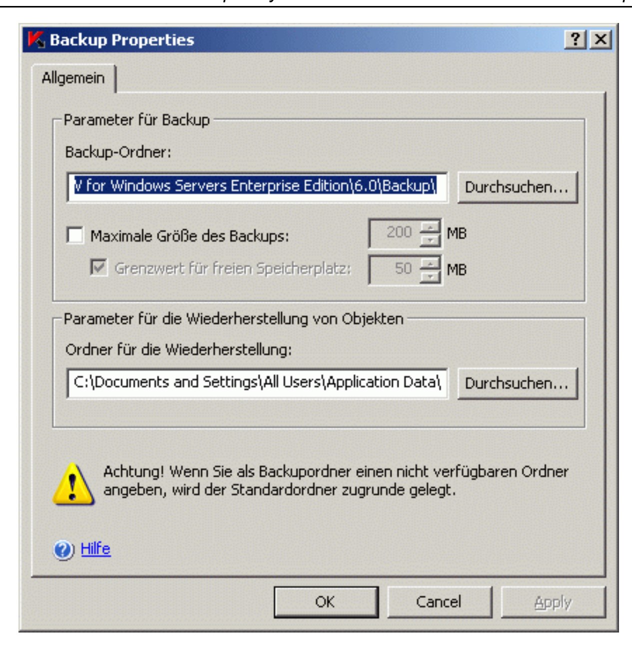


Abbildung 75. Dialogfenster **Eigenschaften : Backup**

2. Im Dialogfenster **Eigenschaften: Backup** machen Sie Folgendes:

   - Um einen Backup-Ordner anzugeben, markieren Sie im Feld **Backup-Ordner** den gewünschten Ordner auf dem lokalen Datenträger des geschützten Servers oder geben Sie dessen Namen und Pfad an (Details zum Parameter finden Sie in Pkt. B.7.1 auf S. 434).

   - Um die maximale Größe des Backups festzulegen, setzen Sie das Häkchen in **Maximale Größe des Backups** und tragen Sie im Eingabefeld den gewünschten Parameterwert in Megabyte ein (s. Pkt. B.7.2 auf S. 435).

   - Um einen Grenzwert für den freien Speicherplatz im Backup festzulegen, wählen Sie den Parameter **Maximale Größe des Backups**, aktivieren Sie das Kontrollkästchen **Grenzwert für freien Speicherplatz** und geben Sie den minimalen Wert für den freien Platz im Backup-Speicher in Megabyte an (s. Pkt. B.7.3 auf S. 435).

   - Um einen Wiederherstellungsordner anzugeben, wählen Sie in der Parametergruppe **Parameter für die Wiederherstellung von Objekten** den gewünschten Ordner auf dem lokalen Datenträger des geschützten Servers oder geben sie im Feld **Ordner für die Wie-**

derherstellung den Namen des Ordners und den vollständigen Pfad ein (s. Pkt. B.7.4 auf S. 436).

3. Klicken Sie auf die Schaltfläche **OK**.

12.6. Statistik für Backup

Sie können Informationen über den aktuellen Status des Backups einsehen, die so genannte *Statistik für Backup*.

*Um die Statistik für Backup anzuzeigen, öffnen Sie in der Konsolenstruktur das Kontextmenü für den Knoten **Backup** und gehen Sie auf den Eintrag **Statistik anzeigen** (s. Abbildung 76).*

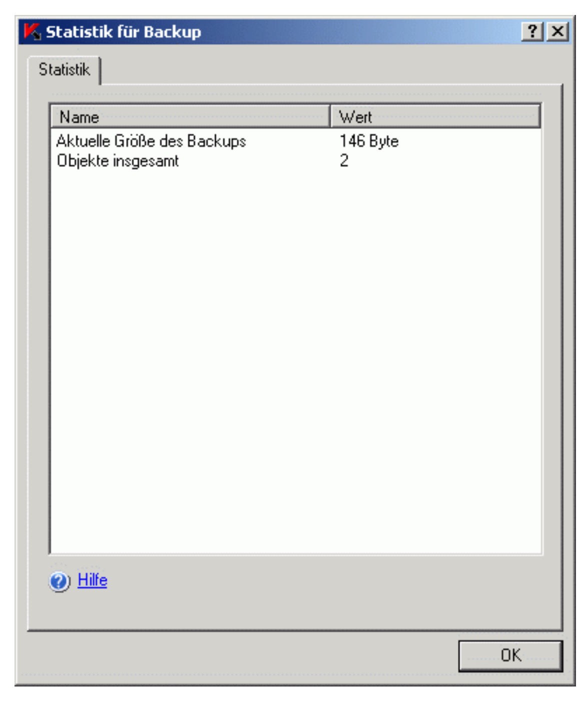


Abbildung 76. Dialogfenster **Statistik für Backup**

Im Dialogfenster **Statistik für Backup** werden die folgenden Informationen über den aktuellen Status des Backups dargestellt:

Tabelle 10. Statistik für Backup

Feld	Beschreibung
Aktuelle Größe des Backups	Datenvolumen im Ordner für den Backup
Objekte insgesamt	Aktuelle Summe der Objekte im Backup

KAPITEL 13. REGISTRIERUNG VON EREIGNISSEN

In diesem Kapitel stehen die folgenden Informationen:

- Registrierung von Ereignissen im Anti-Virus (s. Pkt. 13.1 auf S. 203)
- Berichte über die Aufgabenausführung: Anzeige, Löschen, Einstellen (s. Pkt. 13.2 auf S. 204)
- Bericht zum System-Audit: Anzeige, Leeren (s. Pkt. 13.3 auf S. 218)
- Anti-Virus-Statistik – Informationen über den aktuellen Zustand von Anti-Virus, seiner funktionalen Komponenten und ausführbaren Aufgaben (s. Pkt. 13.4 auf S. 223)
- Event Log des Anti-Virus in der MMC-Konsole "Ereignisanzeige" von Microsoft Windows (s. Pkt. 13.5 auf S. 227)

13.1. Registrierung von Ereignissen

Ereignisse werden im Anti-Virus unterteilt in Ereignisse bei der Objektverarbeitung in den Aufgaben und Ereignisse bei der Anti-Virus-Verwaltung. Darunter fallen solche Ereignisse wie der Start des Anti-Virus, das Anlegen und Löschen von Aufgaben, das Starten von Aufgaben, das Ändern von Aufgabeneinstellungen u.ä.

Anti-Virus registriert Ereignisse auf folgende Weise:

- Er legt *Berichte über die Aufgabenausführung* an. Ein Bericht über die Aufgabenausführung enthält Informationen über den aktuellen Status einer Aufgabe und über Ereignisse, die während der Ausführung eingetreten sind (s. Pkt. 13.2 auf S. 204).
- Er führt ein *Bericht zum System-Audit* zu Ereignissen, die mit der Anti-Virus-Verwaltung zu tun haben (s. Pkt. 13.3 auf S. 218).
- Er trägt eine *Statistik* zusammen, also Informationen über den aktuellen Status der Funktionalkomponenten und Aufgaben, die zurzeit ausgeführt werden (s. Pkt. 13.4 auf S. 223).
- Er führt ein *Ereignisjournal* in der Konsole "Event Viewer von Microsoft Windows", in dem er Ereignisse registriert, die für die Störungsdiagnose wichtig sind (s. Pkt. 13.5 auf S. 227).

Wenn im Betrieb des Anti-Virus Probleme aufgetreten sind (beispielsweise ist Anti-Virus oder eine einzelne Aufgabe abgestürzt) und Sie die Probleme ergründen wollen, können Sie ein *Protokoll der Ablaufverfolgung* und *Speicherauszüge von den Anti-Virus-Prozessen* anlegen und diese Daten zur Analyse an den Technischen Kundendienst von Kaspersky Lab einschicken. Details zum Erstellen eines *Protokolls der Ablaufverfolgung* und zu den *Speicherauszugsdateien* finden Sie in Pkt. 3.2 auf S. 43).

13.2. Berichte über die Aufgabenausführung

In diesem Abschnitt stehen die folgenden Informationen:

- Berichte über die Aufgabenausführung (s. Pkt. 13.2.1 auf S. 204)
- Zusammenfassende Berichte anzeigen (s. Pkt. 13.2.2 auf S. 205)
- Zusammenfassende Berichte sortieren (s. Pkt. 13.2.3 auf S. 209)
- Detailberichte in Aufgaben anzeigen (s. Pkt. 13.2.4 auf S. 210)
- Informationen aus dem Detailbericht in eine Textdatei exportieren (s. Pkt. 13.2.5 auf S. 215)
- Berichte löschen (s. Pkt. 13.2.5 auf S. 215)
- Ändern der Genauigkeitsstufe im Bericht über die Aufgabenausführung einzelner Funktionalkomponenten und im Ereignisjournal (s. Pkt. 13.2.7 auf S. 216)

13.2.1. Berichte über die Aufgabenausführung

Im Knoten **Berichte** können Sie zusammengefasste und detaillierte Berichte über die Ausführung Anti-Virus-Aufgaben anzeigen. *Summenbericht* – Das ist eine Zeile mit Angaben zum Aufgabenstatus und zum Status der verarbeiteten Objekte, die für die Antiviren-Sicherheit interessant sind. Der *Detailbericht* enthält die Statistik über die Aufgabenausführung (Informationen über die Menge der verarbeiteten Objekte), Angaben zu jedem Objekt, das Anti-Virus seit dem Aufgabenstart bis jetzt verarbeitet hat.

Standardmäßig werden Berichte eine begrenzte Zeit lang gespeichert. In Detailberichten über Aufgaben, die zurzeit ausgeführt werden, werden Ereigniseinträge gelöscht, die älter als 30 Tage sind. Ein Summenbericht für eine Aufgabe wird

30 Tage nach der Fertigstellung gelöscht. Sie können mit den Anti-Virus-Parametern die Speicherdauer für Berichte ändern oder die automatische Löschfunktion für Berichte deaktivieren, damit die Einträge uneingeschränkt lange gespeichert werden (s. Kapitel 3 auf S. 43). Sie können einen markierten Bericht auch von Hand löschen.

13.2.2. Summenberichte anzeigen. Status der Summenberichte

Um einen Summenbericht über die Aufgabenausführung anzuzeigen, machen Sie Folgendes:

1. Gehen Sie in der Konsolenstruktur auf den Knoten **Berichte** (s. Abbildung 77).

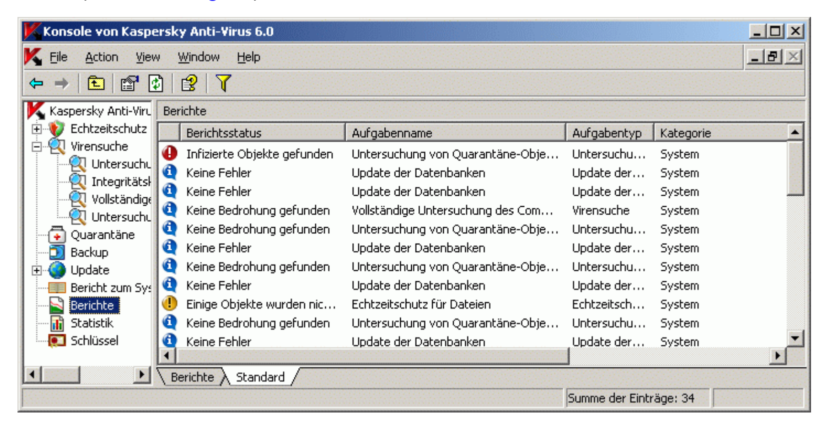


Abbildung 77. Berichtsliste im Ergebnisfenster

2. Im Ergebnisfenster finden Sie den gewünschten Bericht über eine Aufgabe (um einen Bericht in der Liste schnell zu finden, können Sie die Einträge nach dem Inhalt einer beliebigen Spalte filtern oder sortieren lassen.)

   Wie ein Detailbericht über die Aufgabenausführung angezeigt wird, finden Sie in Pkt. 13.2.4 auf S. 210.

Im Bericht stehen die folgenden Informationen über die Aufgabenausführung:

Tabelle 11. Informationen über die Aufgabenausführung im Bericht

Feld	Beschreibung
Berichtsstatus	Summencharakteristik, die anhand der Aufgabenstatistik zusammengestellt wurde. Sie widerspiegelt den aktuellen Status der verarbeiteten Objekte, die für die Antiviren-Sicherheit interessant sind. Die Priorität wird beim Berichtsstatus unterteilt in *informativ* , *Warnung* und *kritisch* . Die Status von Berichten für Aufgaben zur Virensuche und für Updates werden in den folgenden Tabellen beschrieben.
Aufgabenname	Name der Aufgabe, dessen Bericht Sie ansehen
Aufgabentyp	Der Aufgabentyp entspricht der funktionalen Komponente, in der die Aufgabe erstellt wurde (Echtzeitschutz für Dateien, Skript-Untersuchung, Virensuche, Untersuchung von Quarantäne-Objekten, Integritätskontrolle für Anwendungen, Update der Datenbanken, Update der Programm-Module, Update-Verteilung, Rollback des Datenbank-Updates).
Aufgaben-kategorie	*Aufgabenkategorien in Anti-Virus: Systemaufgaben*, *benutzerdefinierte Aufgaben* oder *Gruppenaufgaben*. Details über die Aufgabenkategorien finden Sie in Pkt. 5.1 auf S. 52.
Aufgabenstatus	Aktueller Status der Aufgabe: *Wird ausgeführt*, *Abgeschlossen*, *Angehalten*, *Fehlerhaft abgeschlossen* oder *Vom Benutzer abgebrochen*, *Wird fortgesetzt*.
Abschlusszeit	Wenn die Aufgabe gerade beendet worden ist, wird in dieser Spalte das Datum und die Uhrzeit der Fertigstellung angezeigt. Wenn die Aufgabe gerade ausgeführt wird, bleibt das Feld leer.

Tabelle 12. Status von Berichten über Aufgaben zur Virensuche

Prioritätsstufe	Berichtsstatus	Beschreibung des Berichtsstatus
	Keine Bedrohungen gefunden	Anti-Virus hat alle Objekte im ausgewählten Bereich untersucht. Anti-Virus hat allen untersuchten Objekten den Status *virenfrei* zugewiesen.

Prioritäts-stufe	Berichtsstatus	Beschreibung des Berichtsstatus
!	Einige Objekte wurden nicht verarbeitet	Anti-Virus hat alle untersuchten Objekte als virenfrei identifiziert. Ein oder mehrere Objekte wurden übersprungen, weil sie beispielsweise durch Sicherheitsparameter von der Untersuchung ausgeschlossen wurden oder zum Zeitpunkt des Zugriffs von anderen Programmen verwendet wurden. Zum Zeitpunkt des Zugriffs können beispielsweise Systemdateien von Microsoft Windows nicht verfügbar sein. Sie werden von Anti-Virus nicht untersucht und die Aufgabe wird mit dem Status *Einige Objekte wurden nicht verarbeitet* abgeschlossen.
!	Beschädigte Objekte gefunden	Anti-Virus hat allen untersuchten Objekten den Status nicht infiziert zugewiesen. Eines oder mehrere Objekte wurden im ausgewählten Bereich übersprungen: Anti-Virus konnte diese Objekte nicht lesen, weil deren Format fehlerhaft ist.
!	Verdächtige Objekte gefunden	Anti-Virus hat ein oder mehrere Objekte als verdächtig identifiziert. Sie können im Detailbericht über die Aufgabenausführung feststellen, welche Objekte als verdächtig gelten (s. Pkt. 13.2.4 auf S. 210).
!	Infizierte Objekte gefunden	Anti-Virus hat Bedrohungen in einem oder in mehreren Objekten erkannt. Sie können festlegen, welche Objekte als verdächtig einzustufen sind, indem Sie in den Detailbericht für die Aufgabenausführung (s. Pkt. 13.2.4 auf S. 210) schauen.

Prioritäts-stufe	Berichtsstatus	Beschreibung des Berichtsstatus
	Verarbeitungsfehler	Anti-Virus hat allen untersuchten Objekten den Status nicht infiziert zugewiesen. Während der Untersuchung eines oder mehrerer Objekte ist ein Anti-Virus-Fehler aufgetreten. **Anmerkung** Ein Objekt, bei dessen Verarbeitung ein Fehler des Anti-Virus aufgetreten ist, kann eine Bedrohung enthalten. Es wird empfohlen, dieses Objekt in die Quarantäne zu verschieben und es nach einem Update der Datenbanken erneut zu untersuchen (s. Pkt. 11.3 auf S. 175). Tritt der Fehler noch einmal auf, wenden Sie sich bitte an den Technischen Kundendienst von Kaspersky Lab. Details darüber, wie Sie sich an den Technischen Kundendienst wenden, finden Sie im Anhang A auf S. 373.
	Kritische Fehler	Die Aufgabe wurde mit einem Crash beendet. Sie können den Grund für den Fehler im Detailbericht über die Aufgabenausführung anzeigen.

Tabelle 13. Status von Berichten über Aufgaben zum Update der Datenbanken und zur Update-Verteilung

Prioritäts-stufe	Berichtsstatus	Beschreibung des Berichtsstatus
	Keine Fehler	Anti-Virus hat die Updates empfangen und erfolgreich übernommen.
	Kritische Fehler	Beim Empfang oder Übernehmen von Updates ist ein Fehler aufgetreten. Sie können im Detailbericht über die Aufgabenausführung den Namen des nicht übernommenen Updates und den Grund des Fehlers feststellen.

Tabelle 14. Status von Berichten über Aufgaben zum Update der Programm-Module

Prioritäts-stufe	Berichtsstatus	Beschreibung des Berichtsstatus
	Keine Fehler	Anti-Virus hat die Updates empfangen und erfolgreich übernommen.
	Kritisches Update ist verfügbar	Es wurden dringende Updates für die Anti-Virus-Module veröffentlicht.
	Geplante Updates für Module sind verfügbar	Es wurden planmäßige Updates für die Anti-Virus-Module veröffentlicht.
	Updates für Module sind verfügbar	Es wurden dringende und planmäßige Updates für die Anti-Virus-Module veröffentlicht.
	Updates werden installiert	Anti-Virus hat die Updates empfangen und übernimmt sie.
	Zum Fertigstellen des Update-Vorganges muss der Server neu gestartet werden.	Starten Sie den Server neu, um die Updates zu übernehmen.
	Update wurde nicht ausgeführt	Beim Empfang oder Übernehmen von Updates ist ein Fehler aufgetreten. Sie können im Detailbericht über die Aufgabenausführung den Namen des nicht übernommenen Updates und den Grund des Fehlers feststellen.

13.2.3. Berichte sortieren

Standardmäßig werden Berichte listenförmig in umgekehrter chronologischer Reihenfolge dargestellt. Sie können die Berichte nach dem Inhalt einer Spalte sortieren lassen. Das Sortierergebnis wird gespeichert, wenn Sie den Knoten **Berichte** verlassen und wieder anklicken, oder wenn Sie die Anti-Virus-Konsole mit Speichern in der *msc*-Datei schließen und sie wieder aus dieser Datei wieder öffnen.

Um Berichte zu sortieren, machen Sie Folgendes:

1. Gehen Sie in der Konsolenstruktur auf den Knoten **Berichte**.

2. Im Informationsfenster klicken Sie auf den Spaltenkopf, nach dessen Inhalt Sie die Berichte sortieren wollen.

13.2.4. Detailbericht über Aufgabenausführung anzeigen

Im Detailbericht über die Aufgabenausführung können Sie detaillierte Angaben zu jedem Ereignis anzeigen, das in einer Aufgabe seit dessen Start bis zum jetzigen Augenblick eingetreten ist. So können Sie beispielsweise angeben, in welchem der verarbeiteten Objekt eine Bedrohung erkannt worden ist.

Um einen Detailbericht über die Aufgabenausführung anzuzeigen, machen Sie Folgendes:

1. Gehen Sie in der Konsolenstruktur auf den Knoten **Berichte**.
2. In der Berichtsliste öffnen Sie das Kontextmenü mit einem Rechtsklick auf den Summenbericht der Aufgabe, deren Detailbericht Sie anzeigen wollen, und gehen Sie auf **Bericht anzeigen** und im Dialogfenster öffnen Sie die Registerkarte **Ereignisse**.

Das Dialogfenster **Detailbericht** enthält die Registerkarte **Ereignisse** mit Informationen über die Ereignisse in der Aufgabe, die Registerkarte **Statistik**, auf der die Startzeit, die Abschlusszeit und eine Statistik der Aufgabe angegeben werden, und die Registerkarte **Parameter** mit den Aufgabenparametern.

Die Registerkarte **Ereignisse** enthält folgende Informationen über Ereignisse in der Aufgabe (s. Abbildung 78):

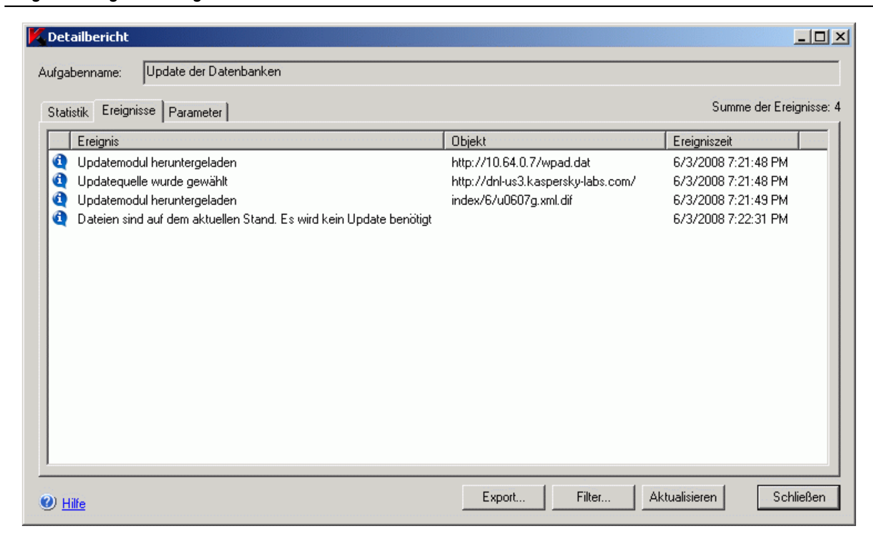


Abbildung 78. Beispiel für Detailbericht über die Aufgabe **Echtzeitschutz für Dateien**

Feld	**Beschreibung**
Prioritätsstufe des Ereignisses	Die Priorität des Ereignisses im Detailbericht wird unterteilt in *informativ* , *wichtig* und *kritisch* .
Ereignisse	Ereignisart und Zusatzinformationen zum Ereignis
Objekt	Name des verarbeiteten Objektes und Pfad In dieser Spalte wird in der Aufgabe **Skript-Untersuchung** auch der PID des Prozesses, der das von Anti-Virus abgefangene Skript ausführte, angezeigt.
Ereigniszeit	Datum und Uhrzeit für Eintreten des Ereignisses

Der Detailbericht über die Aufgabe **Echtzeitschutz für Dateien** enthält außer dem oben genannten Feldern die Felder **Computer** und **Benutzername**. Der Detailbericht über die Aufgabe **Skript-Untersuchung** enthält das Feld **Benutzername**:

Feld	Beschreibung
Computer	Name des Computers, von dem die Anwendung das Objekt abgefragt hat
Benutzername	Name des Benutzers, mit dessen Benutzerkonto die Anwendung auf das Objekt zugegriffen hat Wenn eine Anwendung auf das Objekt zugreifen wollte, die unter dem Benutzerkonto **Lokales System (SYSTEM)** läuft, steht in dieser Spalte der Eintrag <Domäne><Computername>$. In der Aufgabe **Echtzeitschutz für Dateien** registriert Anti-Virus als Computernamen den Wert localhost, und nicht den Netzwerknamen des geschützten Servers, wenn eine Anwendung auf das Objekt zugreift, die auf dem geschützten Server läuft.

*Um die Statistik der Aufgabe anzuzeigen, öffnen Sie im Dialogfenster **Detailbericht** die Registerkarte **Statistik** (s. Abbildung 79).*

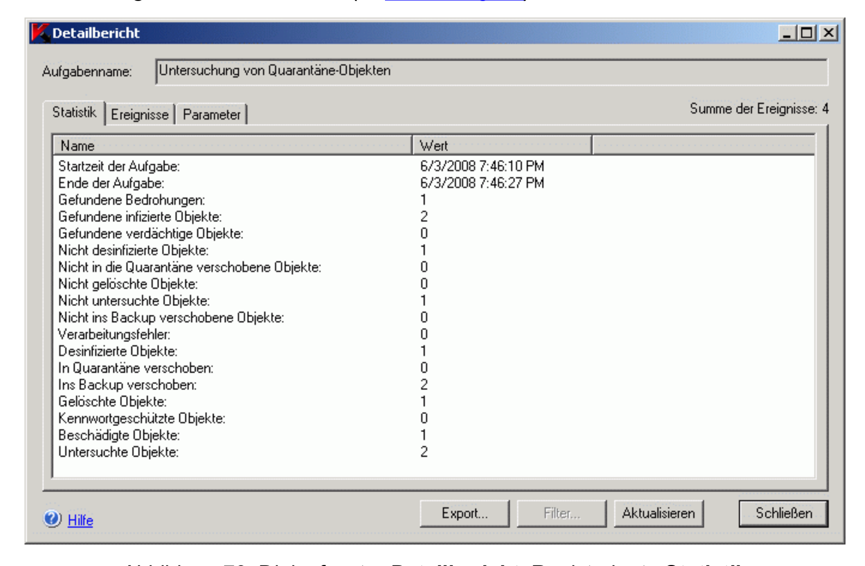


Abbildung 79. Dialogfenster **Detailbericht**, Registerkarte **Statistik**

*Um die Parameter der Aufgabe anzuzeigen, öffnen Sie im Dialogfenster **Detailbericht** die Registerkarte **Parameter** (s. Abbildung 80).*

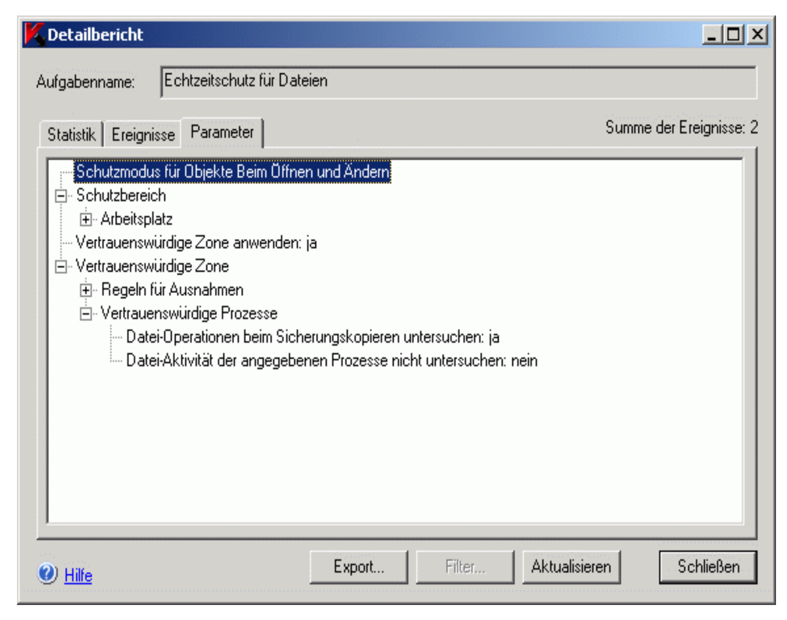


Abbildung 80. Dialogfenster **Detailbericht**, Registerkarte **Parameter**

Wenn Sie den Detailbericht geöffnet haben, können Sie bei der Suche nach einem bestimmten Ereignis auf der Registerkarte **Ereignisse** einen oder mehrere Filter festlegen.

Um einen oder mehrere Filter einzustellen:

1. Klicken Sie im unteren Teil des Dialogfensters **Detailbericht** auf die Schaltfläche **Filter**. Das Dialogfenster **Filterparameter** (s. Abbildung 81) wird geöffnet.

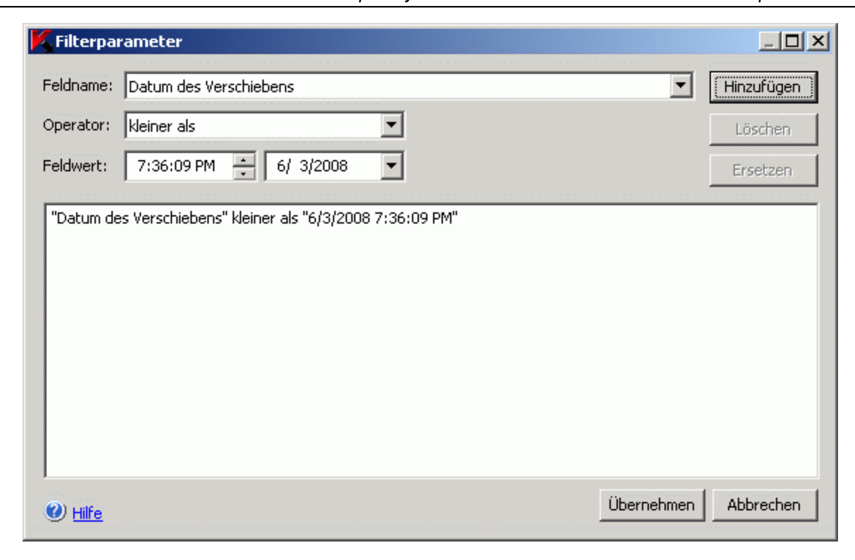


Abbildung 81. Dialogfenster **Filterparameter**

2. Um einen Filter hinzuzufügen:

   a) Wählen Sie in der Liste **Feldname** das Feld, mit dem der Filterwert verglichen wird.

   b) Wählen Sie in der Liste **Operator** eine Filterbedingung. Die Filterbedingungen in der Liste können sich unterscheiden, je nachdem, welchen Wert Sie im Feld **Feldname** wählen.

   c) Geben Sie im Feld **Feldwert** einen Filterwert ein oder wählen Sie einen vorgegebenen Wert aus der Liste.

   d) Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der hinzugefügte Filter wird in der Filterliste im Fenster **Filterparameter** angezeigt. Wiederholen Sie diese Aktionen für jeden Filter, den Sie hinzufügen wollen.

- Um einen Filter zu löschen, markieren Sie den zu entfernenden Filter in der Filterliste und klicken Sie auf **Löschen**.

- Um einen Filter anzupassen, markieren Sie ihn in der Filterliste des Dialogfensters **Filterparameter**, ändern Sie die gewünschten Werte in den Feldern **Feldname**, **Operator** oder **Feldwert**, und klicken Sie auf die Schaltfläche **Ersetzen**.

3. Nachdem Sie alle Filter hinzugefügt haben, klicken Sie auf die Schaltfläche **Übernehmen**. In der Objektliste im Detailbericht werden nun nur

die Objekte dargestellt, die den von Ihnen angegebenen Filtern entsprechen.

*Um wieder alle Objekte anzuzeigen, klicken Sie im unteren Teil des Dialogfensters **Detailbericht** auf die Schaltfläche **Filter** entfernen.*

13.2.5. Export von Informationen aus dem Detailbericht in eine Textdatei

Um Informationen aus dem Detailbericht in eine Textdatei zu exportieren:

1. Wählen Sie in der Konsolenstruktur den Knoten **Berichte**.
2. Öffnen Sie in der Liste der Berichte das Kontextmenü für den Gesamtbericht über die Aufgabe, über deren Ereignisse Sie einen Detailbericht ansehen möchten. Wählen Sie den Befehl **Bericht anzeigen**.
3. Klicken Sie im unteren Bereich des Dialogfensters **Detailbericht** auf die Schaltfläche **Export** und geben Sie im Dialogfenster **Durchsuchen** einen Namen für die Datei an, in der Sie die Informationen aus dem Detailbericht speichern möchten. Geben Sie außerdem die Codierung (Unicode oder ANSI) an.

13.2.6. Berichte löschen

In der Grundeinstellung werden Berichte eine begrenzte Zeit lang gespeichert (Sie können die Aufbewahrungsdauer mit dem allgemeinen Anti-Virus-Parameter **Speichern von Berichten** ändern, s. Pkt. 3.2 auf S. 43).

Im Knoten **Berichte** können Sie markierte Berichte von abgeschlossenen Aufgaben löschen.

Um einen oder mehrere Berichte zu löschen, machen Sie Folgendes:

1. Gehen Sie in der Konsolenstruktur auf den Knoten **Berichte**.
2. Führen Sie eine der Aktionen durch:
   - Um einen Bericht zu löschen, öffnen Sie in der Berichtsliste das Kontextmenü mit einem Rechtsklick auf einen Bericht, den Sie löschen wollen, und gehen Sie auf **Löschen**.
   - Um mehrere Berichte zu löschen, markieren Sie die gewünschten Berichte mit der Taste **<Ctrl>** bzw. **<Shift>**, danach öffnen Sie das Kontextmenü mit einem Rechtsklick auf einen beliebigen Bericht und gehen auf **Löschen**.

Im Dialogfenster **Bestätigung** gehen Sie auf **Ja**, um den Vorgang zu bestätigen. Die ausgewählten Berichte werden gelöscht.

13.2.7. Genauigkeitsstufe für Berichte und Ereignisjournal einstellen

Mithilfe der unten beschriebenen Parameter können Sie vorgeben, welche Ereignisse in den Detailberichten zur Aufgabenausführung der einzelnen Funktionalkomponenten des Anti-Virus registriert werden sollen und welche Ereignisse im Ereignisjournal registriert werden sollen. Details zum Ereignisjournal von Anti-Virus finden Sie in Pkt. 13.5 auf S. 227.

Nach der Priorität werden Ereignisse im Anti-Virus, die mit der Aufgabenausführung zu tun haben, in drei Arten eingeteilt: *Informativ* , *wichtig* und *kritisch* :

Informative Ereignisse, zum Beispiel *Keine Bedrohungen gefunden* oder Keine Fehler, widerspiegeln die Ergebnisse der Anti-Virus-Funktionen.

Wichtige Ereignisse, wie *Fehler bei Verbindung zur Updatequelle*, verlangen vom Administrator Aktionen, können die Funktionalität des Anti-Virus beeinträchtigen.

Kritische Ereignisse können dazu führen, dass die Antiviren-Sicherheit des geschützten Servers in Gefahr gerät. Beispiele dafür sind die Ereignisse *Modul-Integrität ist gestört*, *Bedrohung gefunden* oder *Interner Aufgabenfehler*.

Die Genauigkeitsstufe in den Detailberichten über die Aufgabenausführung und im Ereignisjournal entspricht der Prioritätsstufe der Ereignisse, die darin registriert werden. Sie können eine der drei Genauigkeitsstufen aktivieren, von **Informativ**, bei der Ereignisse aller Prioritätsstufen registriert werden, bis **Kritisch**, bei der nur kritische Ereignisse registriert werden. Standardmäßig gilt die Genauigkeitsstufe **Wichtige Ereignisse** für alle Komponente, außer **Update** (es werden nur wichtige und kritische Ereignisse registriert); für Komponente **Update** ist die Stufe **Informative Ereignisse** definiert.

Sie können manuell einstellen, einzelne Ereignisse in den Detailberichten und im Ereignisjournal registrieren zu lassen.

Um die Genauigkeitsstufe für Ereignisse in den Detailberichten über die Aufgabenausführung und im Ereignisjournal vorzugeben, machen Sie Folgendes:

1. In der Konsolenstruktur öffnen Sie das Kontextmenü für den Knoten **Berichte** und gehen Sie auf den Eintrag **Eigenschaften**.
2. Im Dialogfenster **Eigenschaften: Berichte** (s. Abbildung 82) wählen Sie in der Liste **Komponente** die Funktionalkomponente des Anti-Virus

aus, für deren Aufgabe Sie die Genauigkeitsstufe der Ereignisse eingeben wollen.

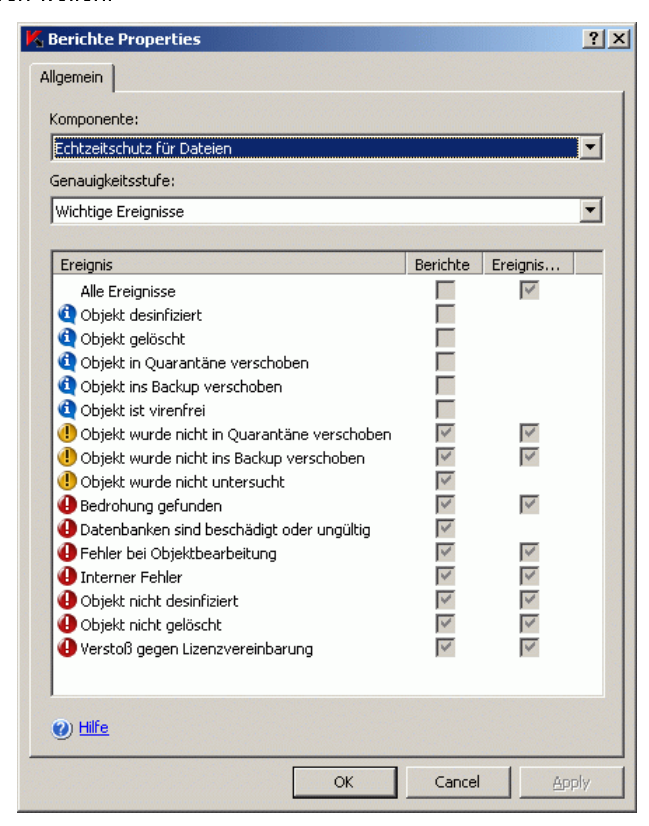


Abbildung 82. Dialogfenster **Eigenschaften: Berichte**

3. Führen Sie eine der Aktionen durch:

   - Um eine Genauigkeitsstufe in den Detailberichten über die Aufgabenausführung einer ausgewählten Funktionalkomponente einzugeben, wählen Sie die gewünschte Stufe in der Liste **Genauigkeitsstufe** aus.

     In der Ereignisliste werden die Häkchen neben den Ereignissen aktiviert, die in den Berichten und im Ereignisjournal je nach der gewählten Genauigkeitsstufe übernommen werden sollen.

   - Um in einen Bericht einzelne Ereignisse der funktionalen Komponente zu übernehmen oder davon auszuschließen, wählen Sie in

der Liste **Genauigkeitsstufe** den Punkt **Benutzereinstellungen**, und danach führen Sie in der Ereignisliste der Komponente die folgenden Aktionen aus:

- Um ein Ereignis in die Detailberichte über die Aufgabenausführung zu übernehmen, setzen Sie das dementsprechende Häkchen in **Berichte**; um ein Ereignis von den Detailberichten auszuschließen, entfernen Sie das dementsprechende Häkchen in **Berichte**.
- Um ein Ereignis in das Ereignisjournal zu übernehmen, setzen Sie das dementsprechende Häkchen in **Ereignisbericht**; um ein Ereignis vom Ereignisjournal auszuschließen, entfernen Sie das dementsprechende Häkchen in **Ereignisbericht**.

4. Klicken Sie auf die Schaltfläche **OK**.

13.3. Bericht zum System-Audit

Anti-Virus führt ein Bericth zum System-Audit für Ereignisse aus, die mit der Anti-Virus-Verwaltung zusammenhängen, wie das Starten des Anti-Virus, das Starten und Beenden von Aufgaben, das Ändern von Aufgabeeinstellungen, das Erstellen und Löschen von Aufgaben zur Virensuche und andere. Die Einträge zu diesen Ereignissen werden im Knoten **Bericht zum System-Audit** dargestellt.

In der Grundeinstellung speichert Anti-Virus Journaleinträge für den Bericht zum System-Audit unbegrenzt lange. Sie können die Aufbewahrungsdauer der Einträge mit dem allgemeinen Anti-Virus-Parameter **Speichern des Berichts zum System-Audit** des System-Audit begrenzen (s. 3.2 auf S. 43).

*Um Ereignisse im Bericht zum System-Audit anzuzeigen, gehen Sie in der Konsolenstruktur auf den Knoten **Bericht zum System-Audit** (s. Abbildung 83).*

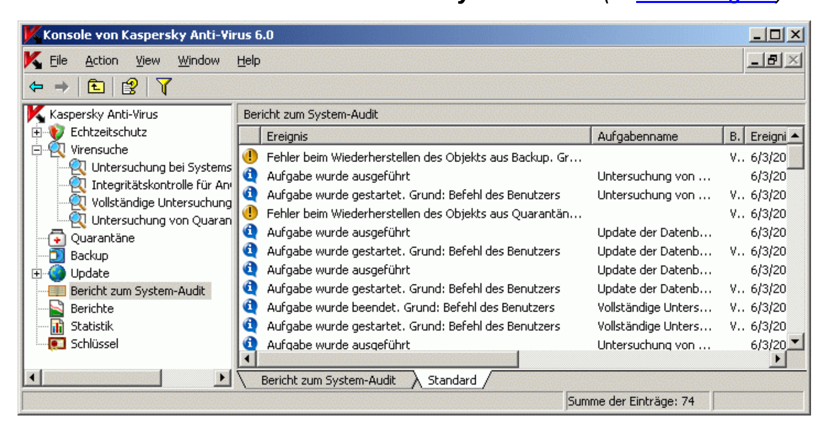


Abbildung 83. Knoten **Bericht zum System-Audit**

Im Ergebnisfenster werden die folgenden Informationen zu jedem Ereignis angezeigt:

Feld	Beschreibung
Ereignis	Beschreibung eines Ereignisses, enthält Ereignisart und Zusatzinformationen. Die Priorität des Ereignisses wird unterteilt in *informativ*, *wichtig* und *kritisch*.
Aufgabenname	Name der Anti-Virus Aufgabe, auf dessen Ausführung sich ein Ereignis bezieht.
Benutzername	Wenn der Anti-Virus-Benutzer ein Ereignis hervorgerufen hat, wird in dieser Spalte der Benutzername angezeigt. Wenn die Aktion nicht der Benutzer, sondern Anti-Virus hervorgerufen hat, er hat beispielsweise die Aufgabe zur Virensuche nach Zeitplan gestartet, steht in der Spalte der Eintrag **<Domäne><Computername>$**, was dem Benutzerkonto **Lokales System** entspricht.
Ereigniszeit	Uhrzeit für die Registrierung des Ereignisses, nach Uhrzeit des Servers im Format, das in den Regionsoptionen von Microsoft Windows eingestellt ist.

Komponente	Funktionalkomponente des Anti-Virus, bei der ein Ereignis aufgetreten ist. Wenn das Ereignis nichts mit den einzelnen Komponenten zu tun hat, sondern mit den Anti-Virus-Funktionen insgesamt, zum Beispiel mit dem Start des Anti-Virus, dann erscheint in dieser Spalte der Eintrag **Anwendung**.
Objekt	Name des Objektes, auf dessen Bearbeitung sich ein Ereignis bezieht (nur für die Komponenten **Quarantäne** und **Backup**).
Computer	Name des Computers, Zugriff von deren zum Server gesperrt oder erlaubt wurde (nur für die Funktion **Zugriff von Computern sperren**).

Sie können die folgenden Aktionen für Ereignisse im Knoten **Bericht zum System-Audit** ausführen:

- Ereignisse sortieren (s. Pkt. 13.3.1 auf S. 220)
- Ereignisse filtern (s. Pkt. 13.3.2 auf S. 221)
- Ereignisse löschen (s. Pkt. 13.3.3 auf S. 222)

13.3.1. Ereignisse im Bericht zum System-Audit sortieren

Standardmäßig werden Ereignisse im Knoten **Bericht zum System-Audit** in umgekehrter chronologischer Reihenfolge dargestellt.

Um ein Ereignis in der Liste zu finden, können Sie die Ereignisse nach dem Inhalt einer Spalte sortieren lassen. Das Sortierergebnis wird gespeichert, wenn Sie den Knoten **Bericht zum System-Audit** verlassen und ihn wieder öffnen, oder wenn Sie die Anti-Virus-Konsole mit Speichern in der *msc*-Datei schließen und sie wieder aus dieser Datei öffnen.

Um Ereignisse zu sortieren, machen Sie Folgendes:

1. Gehen Sie in der Konsolenstruktur auf den Knoten **Bericht zum System-Audit**.
2. Im Ergebnisfenster klicken Sie in der Ereignisliste auf den Spaltenkopf, nach dessen Inhalt Sie die Ereignisse sortieren wollen.

13.3.2. Ereignisse im Bericht zum System-Audit filtern

Um ein Ereignis im Bericht zum System-Audit zu suchen, können Sie die Ereignisse *filtern*, das heißt in der Liste nur die Ereignisse anzuzeigen, die den von Ihnen eingegebenen Filterkriterien (Filtern) entsprechen.

Das Filterergebnis wird gespeichert, wenn Sie den Knoten **Bericht zum System-Audit** verlassen und ihn wieder öffnen, oder wenn Sie die Anti-Virus-Konsole mit Speichern in der *msc*-Datei schließen und sie wieder aus dieser Datei öffnen.

Um Ereignisse im Bericht zum System-Audit zu filtern, machen Sie Folgendes:

1. In der Konsolenstruktur öffnen Sie das Kontextmenü für den Knoten **Bericht zum System-Audit** und gehen Sie auf den Eintrag **Filter**.

   Es öffnet sich das Dialogfenster **Filterparameter** (s. Abbildung 84).

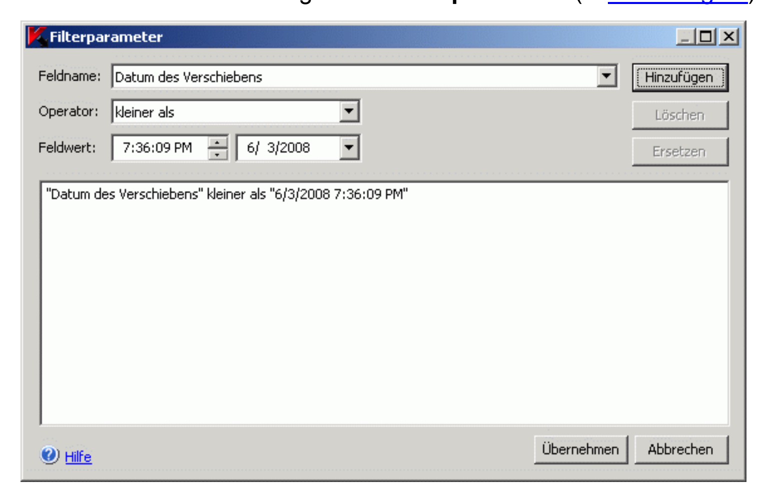


Abbildung 84. Dialogfenster **Filterparameter**

2. Um einen Filter hinzuzufügen, machen Sie Folgendes:

   a) In der Liste **Feldname** wählen Sie ein Feld aus, mit dem der Filterwert verglichen wird.

   b) In der Liste **Operator** wählen Sie die Filterbedingung aus. Die Bedingungswerte für das Filtern können sich voneinander unterscheiden, je nach dem, welchen Wert Sie im Feld **Feldname** ausgewählt haben.

c) Im Feld **Feldwert** geben einen Filterwert ein oder markieren einen Filterwert aus den möglichen Werten.

d) Klicken Sie auf die Schaltfläche **Hinzufügen**.

Der hinzugefügte Filter wird in der Filterliste im Fenster **Suche** dargestellt. Wiederholen Sie diese Vorgänge für jeden Filter, den Sie hinzufügen wollen. Wenn Sie mehrere Filter eingeben, werden sie mit einem logischen UND verknüpft.

3. Um einen Filter zu löschen, markieren Sie den zu entfernenden in der Filterliste und klicken Sie auf die Schaltfläche **Löschen**.

4. Um einen Filter zu bearbeiten, markieren Sie ihn in der Filterliste des Dialogfensters **Filterparameter**, dann ändern Sie die gewünschten Werte in den Feldern **Feldname**, **Operator** oder **Feldwert** und klicken Sie auf die Schaltfläche **Ersetzen**.

5. Nachdem Sie alle Filter hinzugefügt haben, klicken Sie auf die Schaltfläche **Übernehmen**. In der Ereignisliste werden nur die Ereignisse dargestellt, die den von Ihnen eingegebenen Filtern entsprechen.

*Um erneut alle Ereignisse anzuzeigen, öffnen Sie in der Konsolenstruktur das Kontextmenü für den Knoten **Bericht zum System-Audit** und gehen Sie auf den Eintrag **Filter entfernen**.*

13.3.3. Ereignisse aus dem Bericht zum System-Audit löschen

In der Grundeinstellung speichert Anti-Virus Ereignisse im Bericht zum System-Audit unbegrenzt lange. Sie können die Aufbewahrungsdauer für Ereignisse begrenzen (s. Einstellung des Parameters **Speichern des Berichts zum System-Audit** in Pkt. 3.2 auf S. 43).

Sie können manuell alle Ereignisse aus dem Bericht zum System-Audit löschen.

Um alle Ereignisse aus dem Bericht zum System-Audit zu löschen, machen Sie Folgendes:

1. In der Konsolenstruktur öffnen Sie das Kontextmenü für den Knoten **Bericht zum System-Audit** und gehen Sie auf den Eintrag **Leeren**.

2. Im Dialogfenster **Bestätigung** gehen Sie auf **Ja**, um den Vorgang zu bestätigen.

13.4. Anti-Virus-Statistik

Die **Anti-Virus-Statistik** enthält Informationen über den aktuellen Status von Anti-Virus sowie über den Status seiner funktionalen Komponenten und ausführbaren Aufgaben.

*Um die Statistik für Anti-Virus anzuzeigen, wählen Sie in der Konsolenstruktur den Knoten **Statistik**.*

Im Ergebnisfenster werden die folgenden Informationen über den Anti-Virus dargestellt:

- Verweis auf die Anti-Virus-Seite im Internet
- Version und Installationsdatum von Anti-Virus
- Informationen über den aktiven Schlüssel: Seriennummer, Typ, Gültigkeitsdatum und evtl. Informationen über das bevorstehende Ablaufen des Schlüssels

  – Die Gültigkeitsdauer des Schlüssels beträgt mehr als 14 Tage.

  – Die Gültigkeitsdauer des Schlüssels liegt zwischen 7 und 14 Tagen.

  – Die Gültigkeitsdauer des Schlüssels beträgt weniger als 7 Tage.

  Sie können eine Benachrichtigung an den Administrator einstellen, die über das bevorstehende Ende der Gültigkeitsdauer für den Schlüssel informiert (s. Pkt. 15.2 auf S.. 237).
- Status und Parameter der funktionalen Komponenten von Anti-Virus; Status der ausführbaren Aufgaben (siehe Beschreibung in Tabelle 15).

Die Informationen im Knoten **Statistik** werden standardmäßig jede Minute aktualisiert. Sie können die Informationen im Knoten **Statistik** auch auf Befehl aktualisieren.

*Um die Informationen im Knoten **Statistik** manuell zu aktualisieren, öffnen Sie das Kontextmenü für den Knoten **Statistik** und wählen Sie den Befehl **Aktualisieren**.*

Tabelle 15. Informationen über Funktionalkomponenten des Anti-Virus und ausgeführte Aufgaben im Knoten **Statistik**

Komponente/ Aufgabe	Informationen im Knoten Statistik
Echtzeitschutz für Dateien	Status einer Aufgabe: – WIRD AUSGEFÜHRT – Aufgabe wird ausgeführt – BEENDET – Aufgabe ist angehalten oder abgebrochen Aufgabenstatistik: **Gefundene Bedrohungen** – Anzahl der Bedrohungen, die seit dem Aufgabenstart gefunden wurden. **Prophylaxe bei Virenepidemien**: • **Aktiviert** – erhöhte Stufe des Schutzes in der Aufgabe **Echtzeitschutz für Dateien** entsprechend den Parametern der Verhinderung von Virenepidemien (Details finden Sie in Pkt. B.4.4 auf S. 416) • **Deaktiviert** - Verhinderung von Virenepidemien wird nicht angewendet **Untersuchte Objekte** – Anzahl der seit dem letzten Aufgabenstart untersuchten Objekte Wenn die Aufgabe **Echtzeitschutz für Dateien** ausgeführt wird, öffnet der Verweis **Details** das Dialogfenster **Statistik der Aufgabenausführung** (s. Pkt. 6.3 auf S. 91).
Zugriff von Computern sperren	Status von Automatisches Sperren des Zugriffs von Computern: – aktiviert: Verweis **Details** öffnet das Dialogfenster **Statistik** (s. Pkt. 7.9 auf S. 107) – deaktiviert Statistik für Sperrungen: **Computer auf Sperrliste** – Aktuelle Menge an Computern in Sperrliste

Komponente/ Aufgabe	Informationen im Knoten Statistik
Skript-Untersuchung	Status einer Aufgabe: – WIRD AUSGEFÜHRT – Aufgabe wird ausgeführt – BEENDET – Aufgabe ist angehalten oder abgebrochen Aufgabenstatistik: **Gefundene Bedrohungen** – Anzahl der Bedrohungen, die seit dem Aufgabenstart gefunden wurden. **Untersuchte Skripte** – Anzahl der Skripte, die seit dem letzten Aufgabenstart verarbeitet wurden **Gesperrte Skripte** – Anzahl der gefährlichen oder gefährlichen Skripte, die Anti-Virus seit dem Aufgabenstart erkannt und gesperrt hat Wenn die Aufgabe gestartet ist, öffnet der Verweis **Details** das Dialogfenster **Statistik der Aufgabenausführung** (s. Pkt. 6.5 auf S. 95).
Aktualität der Datenbanken	Allgemeiner Status Anti-Virus-Datenbanken auf dem geschützten Server: – Datenbanken sind aktuell – Datenbanken sind veraltet – Datenbanken sind stark veraltet Details zur Aktualität finden Sie in Pkt. 10.1 auf S. 151. **Erstellungsdatum der Datenbanken** – Datum und Uhrzeit für die Erstellung des zuletzt installierten Update der Datenbanken **Einträge in den Datenbanken** – Anzahl der Einträge in den Datenbanken, die zurzeit genutzt werden

Komponente/ Aufgabe	**Informationen im Knoten Statistik**
Informationen zur Quarantäne	Status der Quarantäne (wird dargestellt, wenn die Parameter **Maximale Größe der Quarantäne** und **Grenzwert für freien Speicherplatz** aktiviert sind): – maximale Größe der Quarantäne nicht erreicht; Schwellenwert für freien Speicherplatz in Quarantäne nicht erreicht – maximale Größe der Quarantäne nicht erreicht; aber Schwellenwert für freien Speicherplatz in Quarantäne ist erreicht – Maximale Größe der Quarantäne ist erreicht Wenn das Datenvolumen im Quarantäne-Ordner den in den Parametern angegebenen Wert erreicht, benachrichtigt Anti-Virus den Administrator (wenn Benachrichtigungen für diese Ereignisse eingestellt sind). Anti-Virus verschiebt weiter Objekte in die Quarantäne. Wie Benachrichtigungen eingestellt werden, finden Sie in Kapitel 15 auf S. 235. Wie die Quarantäne-Parameter eingestellt werden, finden Sie in Pkt. 11.8 auf S. 185. Statistik für Quarantäne: **Objekte in Quarantäne** – Anzahl der Objekte, die sich zurzeit in der Quarantäne befinden **Belegter Speicherplatz** – Datenvolumen im Quarantäne-Ordner. Der Verweis **Details** öffnet das Dialogfenster **Statistik für Quarantäne**.

Komponente/ Aufgabe	**Informationen im Knoten Statistik**
Backup	Status des Backups (wird dargestellt, wenn die Parameter **Maximale Größe des Backups** und **Grenzwert für freien Speicherplatz** aktiviert sind): – maximale Größe des Backups nicht erreicht; minimale Größe des freien Speicherplatzes im Backup nicht erreicht – maximale Größe des Backups nicht erreicht; aber Schwellenwert für freien Speicherplatz in Backup ist erreicht – Maximale Größe des Backups ist erreicht Wenn das Datenvolumen im Backup-Ordner den in den Parametern angegebenen Wert erreicht, benachrichtigt Anti-Virus den Administrator (wenn Benachrichtigungen für diese Ereignisse eingestellt sind). Anti-Virus verschiebt weiterhin Datei in den Backup verschieben. Wie Benachrichtigungen eingestellt werden, finden Sie in Kapitel 15 auf S. 235. Wie die Parameter des Backups eingestellt werden, finden Sie in Pkt. 12.5 auf S. 199. Statistik für Backup: **Objekte im Backup** – Anzahl der Dateien, die sich zurzeit im Backup befinden **Belegter Speicherplatz** – Volumen des belegten Speicherplatzes im Backup. Der Verweis **Details** öffnet das Dialogfenster **Statistik für Backup** (s. Pkt. 12.6 auf S. 201).

13.5. Ereignisjournal des Anti-Virus in Konsole "Event Viewer"

Mit der MMC-Konsole von Microsoft Windows "Ereignisanzeige" (Event Viewer) können Sie das Ereignisjournal des Anti-Virus ansehen. In diesem Log registriert Anti-Virus Ereignisse, die aus dem Blickwinkel der Antiviren-Sicherheit des geschützten Servers und der Diagnose von Abstürzen des Anti-Virus wichtig sind.

Sie können Ereignisse auswählen, die im Ereignisjournal registriert werden sollen:

- Nach Ereignistyp;
- nach der Genauigkeitsstufe. Die Genauigkeitsstufe entspricht der Prioritätsstufe von Ereignissen, die im Log registriert werden (*informative*, *wichtige* oder *kritische Ereignisse*). Sehr detailgetreu ist die Stufe *Informativ*, bei der Ereignisse aller Prioritätsstufen registriert werden, nur ungenau ist die Stufe *Kritisch*, bei der nur kritische Ereignisse registriert werden (als Standard ist die Stufe *Wichtige Ereignisse* aktiviert). Standard für alle Komponente außer **Update** ist die Stufe **Wichtige Ereignisse** gesetzt (es werden nur wichtige und kritische Ereignisse registriert); für die Komponente **Update** ist die Stufe **Informative Ereignisse** gesetzt.

Wie Ereignisse zur Registrierung im Ereignisjournal ausgewählt werden, finden Sie in Pkt. 13.2.7 auf S. 216.

Um ein Ereignisjournal anzuzeigen, machen Sie Folgendes:

1. Fügen Sie der MMC-Konsole das Snap-In "Ereignisanzeige" hinzu. Wenn Sie die Serversicherheit im Remote-Betrieb vom Administrator-Arbeitsplatz aus verwalten, geben Sie den geschützten Server als Rechner an, mit dem das Snap-In die Verwaltung ausüben soll.
2. Gehen Sie in der Konsolenstruktur "Ereignisanzeige" auf den Knoten **Ereignisjournal von Kaspersky Anti-Virus 6.0** (s. Abbildung 85).

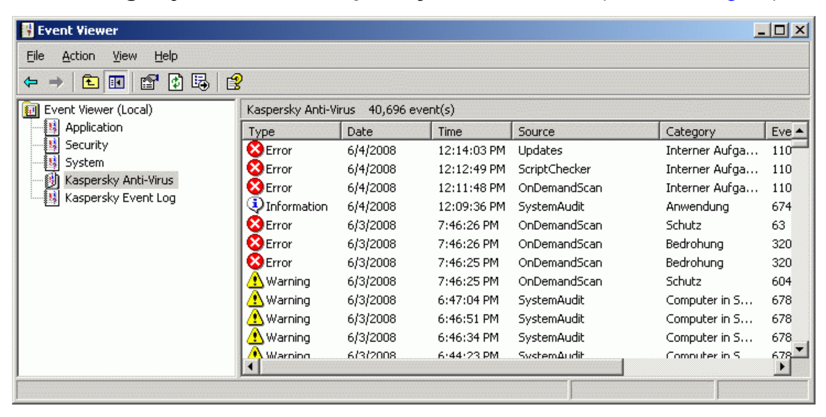


Abbildung 85. Informationen über Ereignisse des Anti-Virus in Konsole "Event Viewer"

KAPITEL 14. AKTIVIERUNG UND DEAKTIVIERUNG VON SCHLÜSSELN

In diesem Kapitel stehen die folgenden Informationen:

- Lizenzschlüssel des Anti-Virus (s. Pkt. 14.1 auf S. 229)
- Informationen über installierte Lizenzschüssel anzeigen (s. Pkt. 14.2 auf S. 231)
- Installation eines Lizenzschlüssels (s. Pkt. 14.3 auf S. 232)
- Löschen eines Lizenzschlüssels (s. Pkt. 14.4 auf S. 234)

14.1. Lizenzschlüssel des Anti-Virus

Der Lizenzschlüssel ist eine Textdatei mit der Dateinamenerweiterung .key. Sie enthält Angaben darüber, welche Berechtigungen und Einschränkungen für den Gebrauch des Anti-Virus herrschen.

Beim Auslesen des Schlüssels wird ein Grenzdatum aktiviert – Datum, *nach dem Verstreichen der Schlüssel ungültig wird*, (zum Beispiel 31. Dezember 2010, wenn die Schlüsseldatei 2007 erstellt wurde). Außerdem wird eine *Funktionsperiode* in Tagen angelegt (zum Beispiel 365 Tage). Kaspersky Lab kann Lizenzschlüssel mit verschiedenen Perioden ausgeben.

Beim Installieren des Lizenzschlüssels errechnet Anti-Virus das *Ablaufdatum für die Gültigkeit des Lizenzschlüssels*. Dieser Termin tritt ein, wenn die Funktionsperiode des Lizenzschlüssels seit seiner Installation verstrichen ist, er liegt aber nicht nach dem Termin, an dem der Schlüssel ungültig wird. Während dieser Frist haben Sie die folgenden Optionen:

- Antiviren-Schutz
- Support mit Datenbanken in der jeweils aktuellen Fassung (Update der Datenbanken)
- Download von kritischen Modul-Updates des Anti-Virus (patch)
- Möglichkeit der Installation von geplanten Updates des Anti-Virus (upgrade)

Im Lauf dieser Frist gewähren Ihnen Kaspersky Lab bzw. seine Fachhändler technische Hilfe, wenn sie in den Bestimmungen für die Schlüsselweitergabe enthalten waren.

Nach dem *Ablaufdatum für die Gültigkeit des Lizenzschlüssels* stellt Anti-Virus die folgenden Funktionen ein: Je nach Schlüssel können Sie entweder nur die Update-Funktion für die Datenbanken und Module des Anti-Virus und die technische Hilfe oder gar keine Anti-Virus-Funktion mehr in Anspruch nehmen.

Im Anti-Virus sind drei Typen für Lizenzschlüssel vorgesehen: *für Beta-Tests*, *Demo-Schlüssel* und *kommerziell*.

Schlüssel für Beta-Tests

Der Schlüssel für Beta-Tests wird kostenlos geliefert. Er ist nur für den Abschnitt gedacht, in dem Anti-Virus die Beta-Testphase durchläuft. Nach dem Verstreichen der Gültigkeit des Lizenzschlüssels stellt Anti-Virus seine Funktionen ein.

Demo-Schlüssel

Der Demo-Schlüssel wird ebenfalls kostenlos geliefert. Er dient dazu, den Anti-Virus näher kennen zu lernen. Der Demo-Schlüssel hat eine sehr kurze Funktionsperiode. Nach dem Verstreichen der Gültigkeit stellt Anti-Virus alle Funktionen ein. Sie können für Anti-Virus nur einen Demo-Schlüssel installieren.

Kommerzieller Schlüssel.

Nach dem Ablauf der Gültigkeit des kommerziellen Lizenzschlüssels führt Anti-Virus alle seine Funktionen aus, außer dem Update. Server wird weiterhin geschützt unter Verwendung der Datenbanken, die vor Ablauf der Gültigkeitsdauer des Schlüssels installiert wurden. Es werden keine Gefahren erkannt, welche von den Kaspersky-Lab-Experten nach Ablauf der Gültigkeitsdauer des Schlüssels in die Datendanken eingetragen wurden und desinfiziert nicht die Objekte, die mit diesen Bedrohungen infiziert sind. Der Technische Kundendienst wird auch nur in der Funktionsperiode des Schlüssels gewährt.

Sie können für das Programm gleichzeitig zwei Schlüssel erwerben und installieren: Ein Schlüssel ist aktiv, der andere Schlüssel liegt auf Reserve. Der *aktive* Schlüssel schaltet das Programm mit seiner Installation sofort frei und der *Reserveschlüssel* tritt automatisch ein, wenn die Gültigkeit des aktiven Schlüssels abgelaufen ist.

Der Anti-Virus-Schlüssel kann eine Einschränkung für dessen Einsatz auf einer bestimmten Menge von Servern haben.

14.2. Informationen über installierte Lizenzschlüssel anzeigen

Um Informationen über die installierten Lizenzschlüssel anzuzeigen, machen Sie Folgendes:

1. Gehen Sie in der Konsolenstruktur auf den Knoten **Schlüssel**.
2. Im Ergebnisfenster öffnen Sie das Kontextmenü mit einem Rechtsklick auf den Schlüssel, den Sie anzeigen wollen, und gehen Sie auf **Eigenschaften**.

   Es öffnet sich das Dialogfenster **Eigenschaften: <Seriennummer des Schlüssels>** (s. Abbildung 86).

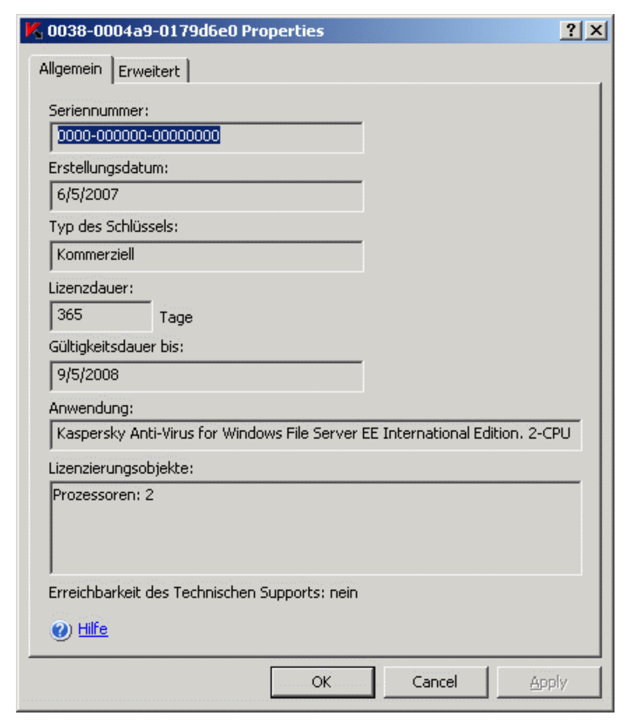


Abbildung 86. Dialogfenster **Eigenschaften: <Seriennummer des Schlüssels>**, Registerkarte **Allgemein**

Im Dialogfenster **Eigenschaften: <Seriennummer des Schlüssels>** werden auf der Registerkarte **Allgemein** die folgenden Informationen angezeigt:

Tabelle 16. Information über den installierten Schlüssel

Feld	Beschreibung
Seriennummer	Seriennummer des Schlüssels
Erstellungsdatum	Datum der Lizenzschlüssel-Erstellung
Typ des Schlüssels	Schlüsseltyp (für Beta-Tests, Demo-Schlüssel oder kommerziell). Details zu den Schlüsseltypen finden Sie in Pkt. 14.1 auf S. 229.
Lizenzdauer	Die Funktionsperiode des Schlüssels in Tagen, wird bei Erstellung des Schlüssels festgelegt
Gültigkeitsdauer bis	Ablaufdatum für die Gültigkeit des Lizenzschlüssels; Anti-Virus errechnet diesen Termin, er tritt ein, wenn die *Funktionsperiode* des Lizenzschlüssels seit seiner Aktivierung verstrichen ist, er liegt aber nicht nach dem *Termin, an dem der Schlüssel ungültig wird*
Anwendung	Anti-Virus-Name
Lizenzierungsobjekte	Wenn im Schlüssel eine Einschränkung hinterlegt ist, werden die Art der Einschränkung und die Menge hier angezeigt.
Erreichbarkeit des Technischen Supports	Informationen darüber, ob Kaspersky Lab bzw. seine Fachhändler dem Kunden Technischen Kundendienst zu den Bestimmungen bei der Schlüsselweitergabe gewähren

Im Dialogfenster **Eigenschaften: <Seriennummer des Schlüssels>** werden auf der Registerkarte **Erweitert** Informationen über den Kunden dargestellt sowie Kontaktangaben von Kaspersky Lab oder des Fachhändlers, von dem Sie Anti-Virus erworben haben.

14.3. Schlüssel installieren

Um einen Schlüssel zu installieren, machen Sie Folgendes:

1. In der Konsolenstruktur öffnen Sie das Kontextmenü für den Knoten **Schlüssel** und gehen Sie auf den Eintrag **Schlüssel installieren**.

2. Im Dialogfenster **Schlüssel hinzufügen** (s. Abbildung 87) geben Sie den Namen der Lizenzschlüsseldatei und den Pfad zur Datei an.

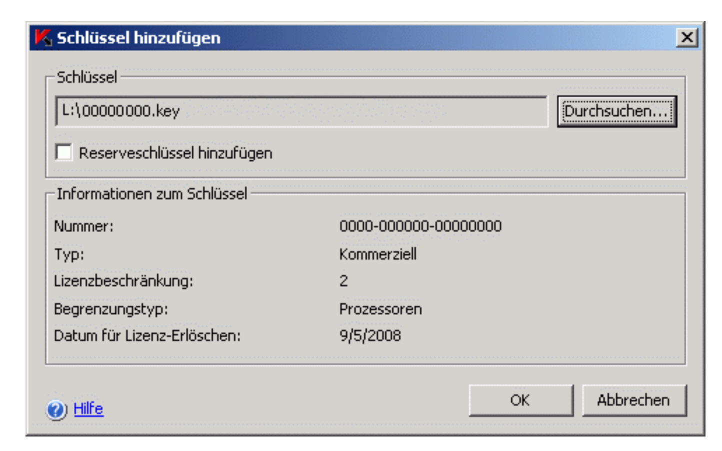


Abbildung 87. Dialogfenster **Schlüssel hinzufügen**

Im Dialogfenster werden die Informationen über den Lizenzschlüssel dargestellt, die in der unten stehenden Tabelle beschrieben sind.

3. Wenn Sie einen Schlüssel als Reserveschlüssel installieren, aktivieren Sie das Kontrollkästchen **Reserveschlüssel hinzufügen**.

4. Klicken Sie auf die Schaltfläche **OK**.

Im Dialogfenster **Schlüssel hinzufügen** wird folgende Information über den installierten Schlüssel angezeigt:

Tabelle 17. Information über den Schlüssel

Feld	Beschreibung
Nummer	Seriennummer des Schlüssels
Schlüsseltyp	Schlüsseltyp (für Beta-Tests, Demo-Schlüssel oder kommerziell). Details zu den Schlüsseltypen finden Sie in Pkt. 14.1 auf S. 229.
Lizenzbeschränkung	Im Lizenzschlüssel angegebene Mengenbeschränkung
Typ der Lizenzbeschränkung	Beschränkungsobjekte

Feld	Beschreibung
Ablaufdatum	*Datum, an dem der Schlüssel ungültig wird*; wird von Anti-Virus berechnet, tritt ein, wenn Schlüsselgültigkeitsperiode von dem Aktivierungsdatum an abläuft, jedoch nicht später als Datum, an dem Schlüssel ungültig wird. Details s. Pkt. 14.1 auf S. 229.

14.4. Schlüssel löschen

Sie können einen installierten Lizenzschlüssel löschen.

Wenn Sie einen aktiven Schlüssel löschen wobei ein Reserve-Schlüssel existiert, wird Reserve-Schlüssel automatisch aktiv.

Achtung!

Wenn Sie einen installierten Lizenzschlüssel löschen, können Sie ihn nur aus einer Schlüsseldatei wiederherstellen.

Um einen installierten Schlüssel zu löschen, machen Sie Folgendes:

1. Gehen Sie in der Konsolenstruktur auf den Knoten **Schlüssel**.
2. Im Ergebnisfenster öffnen Sie das Kontextmenü mit einem Rechtsklick auf die Zeile mit der Information über den Schlüssel, den Sie löschen wollen, und gehen Sie auf **Schlüssel löschen**.
3. Im Dialogfenster klicken Sie auf **Ja**, um den Vorgang des Schlüssellöschens zu bestätigen.

KAPITEL 15. BENACHRICHTIGUNGEN EINSTELLEN

In diesem Kapitel stehen die folgenden Informationen:

- Administrator- und Benutzerbenachrichtigungen (s. Pkt. 15.1 auf S. 235)
- Benachrichtigungen einstellen (s. Pkt. 15.2 auf S. 237)

15.1. Administrator- und Benutzerbenachrichtigung

Anti-Virus kann den Administrator und die Benutzer, die auf den geschützten Server zugreifen, über Ereignisse benachrichtigen, die mit den Funktionen des Anti-Virus und dem Status der Antiviren-Sicherheit des Servers im Zusammenhang stehen:

- Der Administrator kann Informationen über Ereignisse bestimmter Typen erhalten.
- Die Benutzer des lokalen Netzwerkes, die den geschützten Server ansprechen, können Informationen über Ereignisse des Typs *Bedrohung gefunden* und *Computer wurde zur Sperrliste hinzugefügt* erhalten Terminal-Benutzer des Servers können Information über Ereignisse des Typs *Bedrohung gefunden* erhalten.

In der MMC-Konsole des Anti-Virus können Sie die Benachrichtigung des Administrators oder der Benutzer auf verschiedenen Wegen einstellen. Diese Wege sind in den folgenden Tabellen beschrieben.

Tabelle 18. Benutzerbenachrichtigung

Art der Benachrichtigung	**Standardeinstellung**	**Beschreibung**
Fenster für Terminaldienste	Konfiguriert nach Ereignisse des Typs *Bedrohung gefunden*	Wenn der geschützte Server ein Terminal-Server ist, können Sie diese Benachrichtigungsart für die Meldung an die Terminal-Benutzer des Servers anwenden.

Art der Benachrichtigung	Standardeinstellung	Beschreibung
Benachrichtigung mit Messenger von Microsoft Windows	Konfiguriert nach Ereignisse des Typs *Bedrohung gefunden* und *Computer wurde zur Sperrliste hinzugefügt*	Diese Benachrichtigungsart nutzt den Meldeservice von Microsoft Windows. Bevor Sie diese Benachrichtigungsart einsetzen, vergewissern Sie sich, dass der Messenger auf dem geschützten Server und auf den Workstations der Benutzer des lokalen Netzwerkes (als Standard ist er deaktiviert) aktiviert ist.

Tabelle 19. Administratorbenachrichtigung

Art der Benachrichtigung	Standardeinstellung	Beschreibung
Benachrichtigung mit Messenger von Microsoft Windows	nicht konfiguriert	Diese Benachrichtigungsart nutzt den Messenger von Microsoft Windows. Bevor Sie diese Benachrichtigungsart einsetzen, vergewissern Sie sich, dass der Meldeservice auf dem geschützten Server und auf dem Computer aktiviert ist, der die Rolle des Administrator-Arbeitsplatzes (falls der Administrator den Anti-Virus im Remote-Betrieb steuert) spielt. Als Standard ist der Meldeservice deaktiviert.
Starten einer ausführbaren Datei	nicht konfiguriert	Diese Benachrichtigungsart startet nach einem Ereignis, das von einer ausführbaren Datei herrührt. Die ausführbare Datei muss auf dem lokalen Datenträger des geschützten Servers gespeichert sein.
Benachrichtigung per E-Mail	nicht konfiguriert	Diese Benachrichtigungsart nutzt für die Zustellung der Benachrichtigung eine E-Mail.

Sie können einen Nachrichtentext für einzelne Ereignisarten bestimmen. In den Text können Sie Felder mit Angaben zum Ereignis aufnehmen.

Der standardmäßige Nachrichtentext für die Benachrichtigung der Benutzer steht in der folgenden Tabelle.

Tabelle 20. Nachrichtentext für Benutzerbenachrichtigungen in Grundeinstellung

Aufgabe	Ereignisart	Nachrichtentext
Echtzeitschutz für Dateien	*Bedrohung erkannt*	Kaspersky Anti-Virus hat den Zugang zum %OBJECT% auf dem Computer %FROM_COMPUTER% um %EVENT_TIME% gesperrt %FROM_COMPUTER% um %EVENT_TIME% den Zugriff auf %OBJECT% gesperrt. Grund: %EVENT_TYPE%. Bedrohungsart: %VIRUS_TYPE% : %VIRUS_NAME%. Name des Objektbenutzers: %USER_NAME%. Computername des Objektbenutzers: %USER_COMPUTER%
Echtzeitschutz für Dateien, Funktion *Sperren des Zugriffs von Computern*	*Computer in Sperrliste übernommen*	Kaspersky Anti-Virus hat auf dem Computer %FROM_COMPUTER%: %EVENT_TYPE%. Computername: %USER_COMPUTER%. Uhrzeit der Sperrung: %EVENT_TIME%. Grund: Schreibversuch mit infizierten oder verdächtigen Dateien. Wenden Sie sich an den Systemadministrator in Ihrem Netzwerk.

15.2. Benachrichtigungen einstellen

Sollen Benachrichtigungen über Ereignisse eingestellt werden, müssen zunächst die Art der Benachrichtigung und der Inhalt der Textnachricht festgelegt sein.

Um Benachrichtigungen über Ereignisse einzustellen, machen Sie Folgendes:

1. Öffnen Sie in der Konsolenstruktur das Kontextmenü des Anti-Virus-Snap-Ins und gehen Sie auf **Benachrichtigungen einstellen**.

   Es öffnet sich das Dialogfenster **Benachrichtigungen** (s. Abbildung 88).

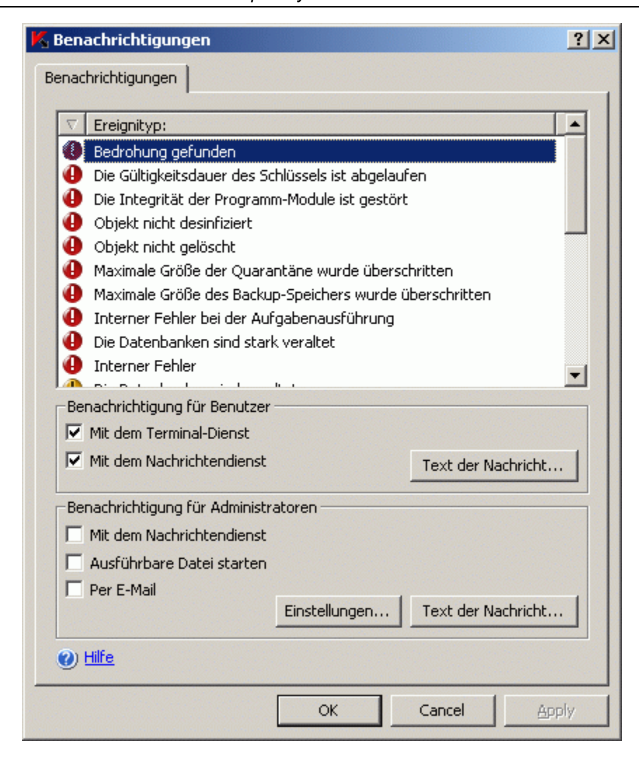


Abbildung 88. Dialogfenster **Benachrichtigungen**

2. Im Dialogfenster **Benachrichtigungen** markieren Sie auf der Registerkarte **Benachrichtigungen** die Ereignisse und geben Sie die Art der Benachrichtigung an:

   - Um Benachrichtigungsarten für einen Administrator auszuwählen, führen Sie die folgenden Aktionen aus:

     a) In der Liste **Ereignistyp** wählen Sie ein Ereignis aus, für das Sie die Benachrichtigungsart bestimmen wollen.

     b) In der Parametergruppe **Benachrichtigung für Administratoren** setzen Sie das Häkchen neben den Benachrichtigungsarten, die Sie einstellen wollen.

   - Um Benachrichtigungsarten für Benutzer auszuwählen, führen Sie die folgenden Aktionen aus:

     a) Wählen Sie **Ereignistyp** (*Bedrohung gefunden* und *Computer wurde zur Sperrliste hinzugefügt*), über welchen Sie die Benut-

zer benachrichtigen wollen, auf Computer deren diese Ereignisse auftreten.

b) In der Parametergruppe **Benachrichtigung für Benutzer** setzen Sie das Häkchen neben den Benachrichtigungsarten, die Sie einstellen wollen.

> **Anmerkung**
>
> Sie können einen Nachrichtentext für mehrere Ereignisarten bestimmen: Nachdem Sie die Benachrichtigungsart für eine Ereignisart ausgewählt haben, entscheiden Sie sich mit den Tasten **<Ctrl>** bzw. **<Shift>** für die anderen Ereignisarten, für die Sie den gleichen Nachrichtentext erzeugen wollen.

3. Um einen Nachrichtentext zu erstellen, klicken Sie auf die Schaltfläche **Text der Nachricht** in der gewünschten Parametergruppe und im Dialogfenster **Text der Nachricht** geben Sie den Text ein, der in der Nachricht zum Ereignis dargestellt werden soll.

   Um ein Feld mit Informationen zum Ereignis hinzuzufügen, klicken Sie auf die Schaltfläche **Makros** und wählen Sie die gewünschten Felder aus den möglichen Werten aus. Felder mit Ereignisinformationen werden in der Tabelle 21 näher beschrieben.

   Um den Text wiederherzustellen, der standardmäßig für Ereignisse vorgesehen ist, klicken Sie auf die Schaltfläche **Grundeinstellung**.

4. Um die ausgewählten Benachrichtigungsarten für Administratoren einzustellen, klicken Sie im Dialogfenster **Benachrichtigungen** auf die Schaltfläche **Einstellungen** und im Dialogfenster **Erweiterte Einstellungen** führen Sie die Einstellung der gewählten Arten aus.

   - Für Benachrichtigungen per E-Mail öffnen Sie die Registerkarte **E-Mail** (s. Abbildung 89) tragen Sie in die entsprechenden Felder die E-Mail-Adresse der Empfänger (trennen Sie die Adressen durch Semikolon), den Namen oder die Netzwerk-Adresse des SMTP-Servers sowie dessen Port ein. Bei Bedarf tragen Sie den Text ein, der in den Feldern **Betreff** und **Von** zu sehen sein soll. In den Text des Feldes **Betreff** können Sie Felderwerte mit Informationen zum Ereignis aufnehmen (s. Tabelle 21).

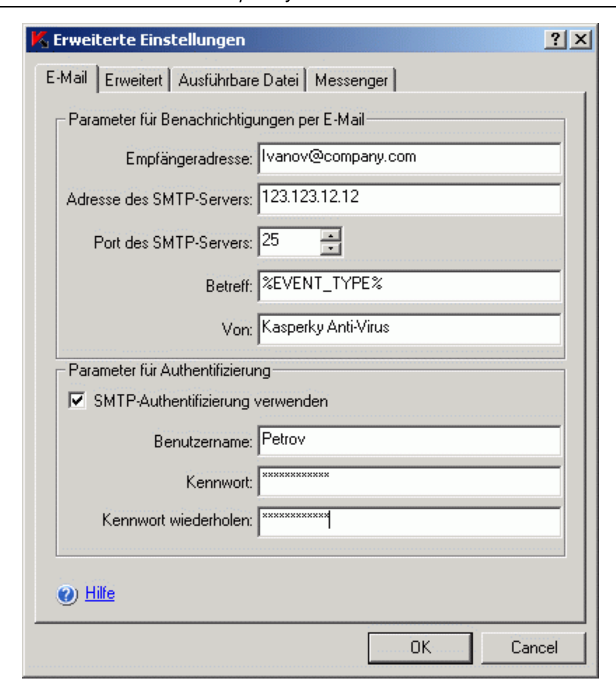


Abbildung 89. Dialogfenster **Erweiterte Einstellungen**, Registerkarte **E-Mail**

Wenn Sie das Benutzerkonto bei der Verbindung mit dem SMTP-Server authentifizieren wollen, setzen Sie in der Gruppe **Parameter für Authentifizierung** das Häkchen in **SMTP-Authentifizierung verwenden** und tragen Sie den Namen und das Kennwort des Benutzers ein, dessen Benutzerkonto Sie prüfen lassen wollen.

- Zur Benachrichtigung über den Messenger erstellen Sie auf der Registerkarte **Messenger** (s. Abbildung 90) eine Liste mit den Rechnern, die Benachrichtigungen empfangen sollen: Für jeden hinzuzufügenden Computer klicken Sie auf die Schaltfläche **Hinzufügen** und im Eingabefeld tragen Sie dessen Netzwerknamen ein. Geben Sie in diesem Feld keine IP-Adressen der Rechner ein.

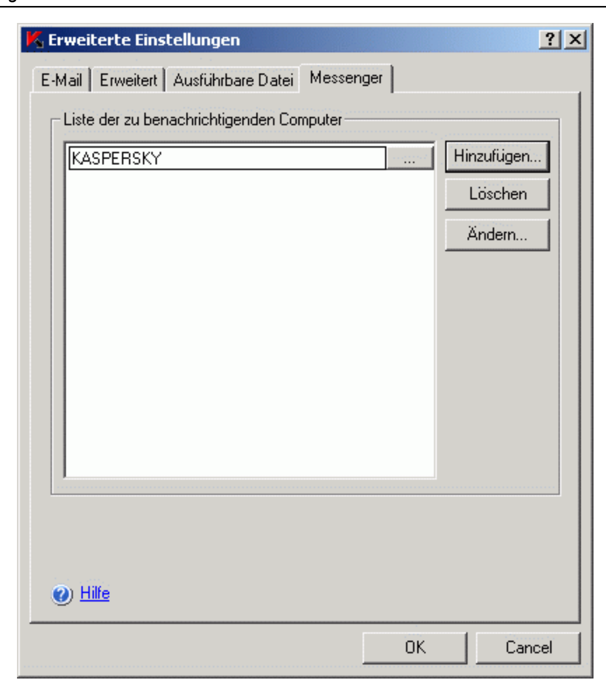


Abbildung 90. Dialogfenster **Erweiterte Einstellungen**, Registerkarte **Messenger**

- Für den Start einer ausführbaren Datei wählen Sie auf der Registerkarte **Ausführbare Datei** (s. Abbildung 91) auf dem lokalen Datenträger des geschützten Servers die Datei aus, die nach Eintreten des Ereignisses auf dem Server gestartet werden soll, oder geben Sie den vollständigen Pfad zu dieser Datei ein. Tragen Sie den Namen und das Kennwort des Benutzers ein, unter dessen Benutzerkonto die Datei auszuführen ist.

  Wenn Sie den Pfad zu der ausführbaren Datei angeben, können Sie die Umgebungsvariablen des Systems verwenden. Dagegen können Sie die benutzerdefinierten Umgebungsvariablen nicht verwenden.

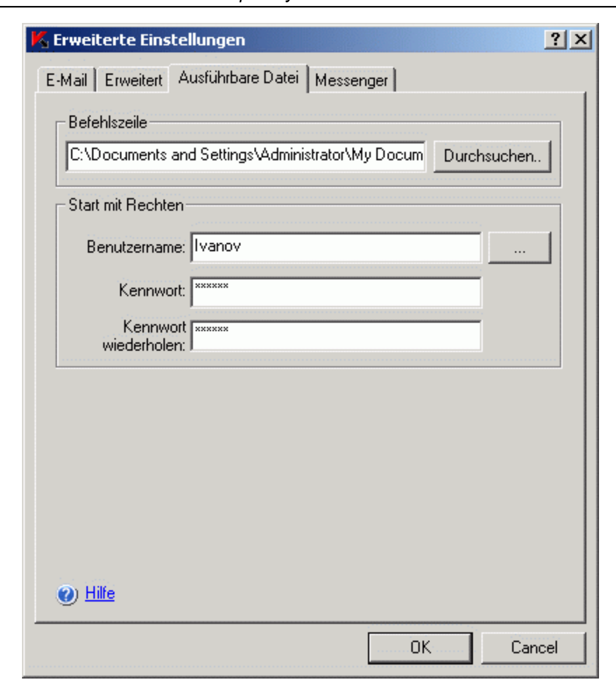


Abbildung 91. Dialogfenster **Erweiterte Einstellungen**, Registerkarte **Ausführbare Datei**

- Wenn Sie die Anzahl der Benachrichtigungen nach Ereignissen einer Art je Zeiteinheit begrenzen wollen, setzen Sie auf der Registerkarte **Erweitert** (s. Abbildung 92) das Häkchen im Kontrollkästchen **Eine Benachrichtigung nicht häufiger senden als** und tragen Sie die gewünschte Menge je Zeiteinheit ein.

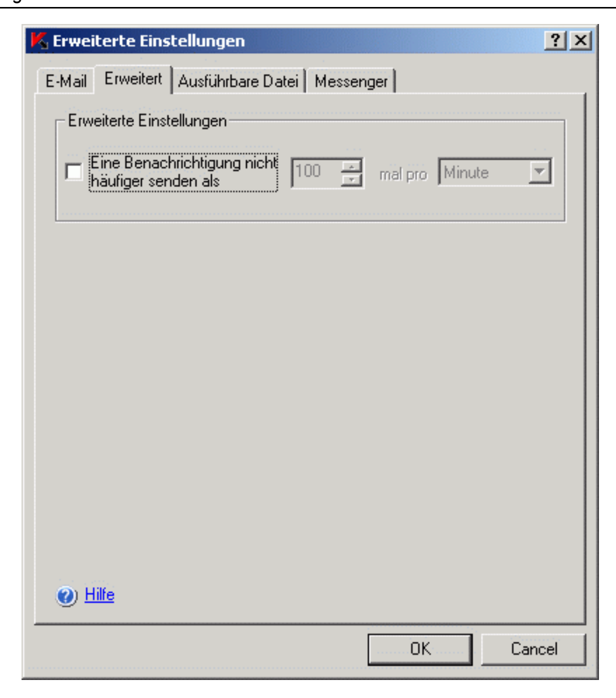


Abbildung 92. Dialogfenster **Erweiterte Einstellungen**, Registerkarte **Erweitert**

5. Klicken Sie auf die Schaltfläche **OK**.

Tabelle 21. Felder mit Ereignisinformationen

Feld	Beschreibung
%EVENT_TYPE%	Ereignisart
%EVENT_TIME%	Uhrzeit bei Eintreten des Ereignisses
%EVENT_SEVERITY%	Prioritätsstufe des Ereignisses
%OBJECT%	Name des Objektes (in den Aufgaben des Echtzeitschutzes und zur Virensuche) In der Aufgabe **Update der Programm-Module** stehen der Name des Updates und die Adresse der Internetseite mit näheren Angaben zum Update.

Feld	Beschreibung
%VIRUS_NAME%	Name der Bedrohung nach der Klassifizierung von Kaspersky Lab, gehört zur vollständigen Bezeichnung einer Bedrohung, die Anti-Virus meldet (in den Aufgaben des Echtzeitschutzes und zur Virensuche)
%VIRUS_TYPE%	Typ der Bedrohung nach der Klassifizierung von Kaspersky Lab, gehört zur vollständigen Bezeichnung einer Bedrohung, die Anti-Virus meldet (in den Aufgaben des Echtzeitschutzes und zur Virensuche)
%USER_COMPUTER%	In der Aufgabe **Echtzeitschutz für Dateien** Name des Computerbenutzers, der über den Server auf ein Objekt zugegriffen hat
%USER_NAME%	In der Aufgabe **Echtzeitschutz für Dateien** Name des Benutzers, der über den Server auf ein Objekt zugegriffen hat
%FROM_COMPUTER%	Name des geschützten Servers, von dem die Benachrichtigung eingegangen ist
%REASON%	Grund für Eintreten eines Ereignisses (einige Ereignisse haben dieses Feld nicht)
%ERROR_CODE%	Fehlercode (gilt nur für das Ereignis *interner Aufgabenfehler*)
%TASK_NAME%	Name der Aufgabe (nur für Ereignisse, die mit der Aufgabenausführung verbunden sind)

TEIL 2. VERWALTUNG VON ANTI-VIRUS AUS DER BEFEHLSZEILE

In diesem Abschnitt stehen die folgenden Informationen:

- Beschreibung der Administrationsbefehle für den Anti-Virus aus der Befehlszeile (s. Kapitel 16 auf S. 246)
- Beschreibung der Feedback-Codes (s. Kapitel 17 auf S. 268)

KAPITEL 16. VERWALTUNG DES ANTI-VIRUS AUS DER BEFEHLSZEILE

Sie können die Basisbefehle für die Steuerung des Anti-Virus aus der Befehlszeile des geschützten Servers heraus erteilen, wenn Sie bei der Installation des Anti-Virus in der Liste der zu installierenden Komponenten **Befehlszeilen-Utility** mit angekreuzt haben.

Mithilfe von Befehlszeilen-Befehlen können Sie nur die Funktionen benutzen, welche für Sie entsprechend Ihren Rechten im Anti-Virus zugängig sind (Details dazu lesen Sie in Pkt. 2.6.1 auf S. 37).

Einige Befehle des Anti-Virus werden synchron ausgeführt: Die Steuerung greift auf die Konsole erst zurück, wenn ein Befehl abgearbeitet wurde, andere Befehle erfolgen asynchron: Die Steuerung greift sofort nach dem Befehlsstart auf die Konsole zurück.

Um einen Befehl synchron zu unterbrechen, klicken Sie zusammen auf **<Ctrl+C>**.

Bei der Eingabe Anti-Virus-Befehle gelten die folgenden Regeln:

- Geben Sie Schlüssel und Befehle mit Zeichen des oberen oder unteren Registers ein.
- Trennen Sie Schlüssel mit Leerzeichen voneinander.
- Wenn der Name einer Datei (eines Ordners), deren (dessen) Pfad Sie als Schlüsselwert eingeben, ein Leerzeichen enthält, schließen Sie den Pfad zur Datei (zum Ordner) in Anführungszeichen ein, zum Beispiel: "C:\TEST\test cpp.exe”.
- In den Masken der Datei- und Pfadnamen setzen Sie nur ein Auslassungszeichen ein, und geben Sie diesen nur am Ende des Pfades zur Datei oder Verzeichnis, y. B.: "C:\Temp\Temp*\", "C:\Temp\Temp???.doc", "C:\Temp\Temp*.doc"

Eine Liste mit den Befehlen des Anti-Virus steht in Tabelle 22.

Die Feedback-Codes des Anti-Virus stehen in Kapitel 17 auf S. 268.

Tabelle 22. Anti-Virus-Befehle

Befehl	**Beschreibung**
KAVSHELL HELP (16.1)	Aufrufen der Hilfe für Anti-Virus-Befehle
KAVSHELL START (16.2)	Starten des Anti-Virus-Dienstes
KAVSHELL STOP (16.2)	Beenden des Anti-Virus-Dienstes
KAVSHELL SCAN (16.3)	Erstellen und Starten der zeitweiligen Aufgabe zur Virensuche mit einem Untersuchungsbereich und Parametern für Sicherheit, die von den Befehlsschlüsseln vorgegeben werden
KAVSHELL FULLSCAN (16.4)	Starten der Systemaufgabe **Vollständige Untersuchung des Computers**
KAVSHELL TASK (16.5)	asynchrones Starten/Anhalten/Fortsetzen/Beenden der angegebenen Aufgabe / Meldung des aktuellen Aufgabenstatus / Statistik der Aufgabenausführung
KAVSHELL RTP (16.6)	Starten oder Beenden aller Aufgaben des Echtzeitschutzes
KAVSHELL UPDATE (16.7)	Starten der Aufgabe Update der Anti-Virus-Datenbanken mit den Befehlszeilen-Parametern
KAVSHELL ROLLBACK (16.8)	Rollback der Datenbanken auf die Vorgänger-Version
KAVSHELL LICENSE (16.9)	Verwaltung der Lizenzschlüssel
KAVSHELL TRACE (16.10)	Aktivieren oder Deaktivieren von Einträgen in das Protokoll der Ablaufverfolgung, Verwalten der Parameter für das Protokoll der Ablaufverfolgung
KAVSHELL DUMP (16.11)	Aktivieren oder Deaktivieren der Erstellung eines Speicherauszuges von einem Prozess bei dessen anomalen Beenden
KAVSHELL IMPORT (16.12)	Importieren der allgemeinen Anti-Virus-Parameter, dessen Funktionen und Aufgaben aus der zuvor erstellten Konfigurationsdatei
KAVSHELL EXPORT (16.13)	Exportieren aller Anti-Virus-Parameter und aller vorhandenen Aufgaben in eine Konfigurationsdatei

16.1. Aufrufen Anti-Virus-Befehle. KAVSHELL HELP

Um eine Liste mit allen Anti-Virus-Befehlen auszugeben, geben Sie einen der folgenden Befehle ein:

```
KAVSHELL
KAVSHELL HELP
KAVSHELL /?
```

Um eine Beschreibung und die Syntax aller Anti-Virus-Befehle zu beziehen, geben Sie einen der folgenden Befehle ein:

```
KAVSHELL HELP <Befehl>
KAVSHELL <Befehl> /?
```

Beispiele für den Befehl KAVSHELL HELP

`KAVSHELL SCAN SCAN` – Anzeigen von detaillierten Informationen zum Befehl KAVSHELL SCAN.

16.2. Anti-Virus-Dienst starten und beenden. KAVSHELL START, KAVSHELL STOP

Um den Anti-Virus-Dienst zu starten, verwenden Sie den Befehl KAVSHELL START.

> **Anmerkung**
>
> Standardmäßig werden beim Start von Anti-Virus Aufgaben **Echtzeitschutz für Dateien**, **Skript-Untersuchung**, **Überprüfung bei Systemstart** und **Integritätskontrolle für Anwendungen**, wie auch andere Aufgaben, in dem Zeitplan welchen die Häufigkeit **Bei Programmstart** angegeben ist.

Um den Anti-Virus-Dienst zu beenden, verwenden Sie den Befehl KAVSHELL STOP.

16.3. Angegebenen Bereich untersuchen. KAVSHELL SCAN

Um die Aufgabe Untersuchung von einzelnen Bereichen des geschützten Servers zu starten, verwenden Sie den Befehl KAVSHELL SCAN. Die Befehlsschlüssel geben die Aufgabenparameter (Untersuchungsbereich und Parameter für Sicherheit) vor.

Die Aufgabe zur Virensuche, die mit dem Befehl KAVSHELL SCAN gestartet worden ist, ist *temporär*. Er wird in der Anti-Virus-Konsole der MMC nur während der Ausführung angezeigt (in der Anti-Virus-Konsole können Sie die Parameter der Aufgabe nicht ansehen). Gleichzeitig wird ein Bericht über die Aufgabenausführung registriert und im Knoten **Berichte** der Anti-Virus-Konsole dargestellt. Ebenso wie für die Aufgaben zur Virensuche, die in der Anti-Virus-Konsole angelegt worden sind, können für Aufgaben, die mit dem Befehl SCAN angelegt und gestartet werden, die Richtlinien des Programms Kaspersky Administration Kit angewendet werden (Details zur Verwendung von Kaspersky Administration Kit für die Verwaltung des Anti-Virus finden Sie in Kapitel 3 auf S. 43).

Der Befehl KAVSHELL SCAN wird synchron ausgeführt.

Wenn Sie in der Aufgabe Virensuche Pfade eingeben, können Sie keine Umgebungsvariablen verwenden. Verwenden Sie eine Umgebungsvariable, die für einen Benutzer bestimmt ist, geben Sie das Kommando KAVSHELL SCAN mit den Berechtigungen dieses Benutzers ein.

Um eine vorhandene Aufgabe zur Virensuche aus der Befehlszeile zu starten, verwenden Sie den Befehl KAVSHELL TASK (s. Pkt. 16.5 auf S. 255).

Syntax des Befehls KAVSHELL SCAN

```
KAVSHELL SCAN  [Untersuchungsbereich
/MEMORY|/SHARED|/STARTUP|/REMDRIVES|/FIXDRIVES|/MYCOMP]
[/L:< Pfad zur Datei mit Liste der Untersuchungsbereiche >]
[/F<A|C|E>] [/NEWONLY]
[/AI:<DISINFECT|DISINFDEL|DELETE|REPORT|AUTO>]
[/AS:<QUARANTINE|DELETE|REPORT|AUTO>] [/DISINFECT|/DELETE]
[/E:<ABMSPO>] [/EM:<"Masken">] [/ES:<Größe>] [/ET:<Anzahl
der Sekunden>] [/ICHECKER][/ISWIFT][/W:<Pfad zur Protokoll-
datei>] [/ALIAS:<Alias des Aufgabenamen>]
```

Beispiele für den Befehl KAVSHELL SCAN

```
KAVSHELL SCAN Folder4 D:\Folder1\Folder2\Folder3\
C:\Folder1\ C:\Folder2\3.exe "\\server1\Shared Folder\"
F:\123\*.fgb /SHARED /AI:DISINFDEL /AS:QUARANTINE /FA
```

```
/E:ABM /EM:"*.xtx;*.ff?;*.ggg;*.bbb;*.info" /NOICHECKER
/NOISWIFT /W:report.log
KAVSHELL SCAN  /W:log.log
```

<table>
<tr><th>Schlüssel</th><th>Beschreibung</th></tr>
<tr><td colspan="2">Untersuchungsbereich. Pflichtschlüssel</td></tr>
<tr><td><Dateien></td><td rowspan="3">Untersuchungsbereich – eine Liste aus Dateien, Ordnern, Netzwerkpfaden und vordefinierten Bereichen
Tragen Sie die Netzwerkpfade im UNC-Format (Universal Naming Convention) ein.
Im folgenden Beispiel wurde der Ordner Folder4 ohne Pfad eingegeben – er befindet sich im Verzeichnis, aus welchen das Befehl KAVSHELL gestartet wird:
KAVSHELL SCAN Folder4</td></tr>
<tr><td><Ordner></td></tr>
<tr><td><Netzwerkpfad></td></tr>
<tr><td>/MEMORY</td><td>Objekte im Arbeitsspeicher untersuchen</td></tr>
<tr><td>/SHARED</td><td>Gemeinsame Ordner auf dem Server untersuchen</td></tr>
<tr><td>/STARTUP</td><td>Autostart-Objekte untersuchen</td></tr>
<tr><td>/REMDRIVES</td><td>Wechseldatenträger untersuchen</td></tr>
<tr><td>/FIXDRIVES</td><td>Festplatten-Datenträger untersuchen</td></tr>
<tr><td>/MYCOMP</td><td>Alle Bereiche des geschützten Servers untersuchen</td></tr>
<tr><td>/L: <Pfad zur Datei mit Liste der Untersuchungsbereiche></td><td>Name der Datei mit Liste der Untersuchungsbereiche mit vollständigem Pfad zur Datei
Untersuchungsbereiche in der Datei teilen Sie mit Zeilenumbrüchen voneinander. Sie können vordefinierte Untersuchungsbereiche angeben, wie im folgenden Beispiel für eine Textdatei mit einer Liste von Untersuchungsbereichen:
C:\
D:\Docs*.doc
E:\Docs\
/STARTUP
/SHARED</td></tr>
<tr><td colspan="2">Zu untersuchende Objekte (File types). Wenn Sie keine Werte für diesen Schlüssel angeben, untersucht Anti-Virus Objekte nach Format.</td></tr>
</table>

Schlüssel	Beschreibung
/FA	Alle Objekte untersuchen
/FC	Objekte nach Format untersuchen (Standard). Es werden nur die Objekte vom Anti-Virus untersucht, deren Formate zu infizierenden Objekten entsprechen.
/FE	Objekte nach Erweiterung untersuchen. Es werden nur die Objekte vom Anti-Virus untersucht, deren Formate zu infizierenden Objekten entsprechen.
/NEWONLY	Nur neue und veränderte Dateien untersuchen (Details zu diesem Parameter s. in Pkt. B.3.2 auf S. 397). Wenn Sie diesen Schlüssel nicht angeben, wird Anti-Virus alle Objekte untersuchen.
/AI: **Aktionen für infizierte Objekte**. Wenn Sie keine Werte für diesen Schlüssel angeben, führt Anti-Virus die Aktion **Überspringen** aus.	
DISINFECT	Desinfizieren, wenn eine Desinfektion nicht möglich ist, überspringen
DISINFDEL	Desinfizieren, wenn eine Desinfektion nicht möglich ist, löschen
DELETE	Löschen
REPORT	Überspringen (Standard)
AUTO	Empfohlene Aktion ausführen
/AS: **Aktionen für verdächtige Objekte** (actions). Wenn Sie keine Werte für diesen Schlüssel angeben, führt Anti-Virus die Aktion **Überspringen** aus.	
QUARANTINE	In Quarantäne verschieben
DELETE	Löschen
REPORT	Überspringen (Standard)
AUTO	Empfohlene Aktion ausführen
Ausnahmen (Exclusions)	

Schlüssel	Beschreibung
/E:ABMSPO	Ausschließen von Compound-Objekten der folgenden Art: A – Archive B – Mail-Datenbanken M – Dateien in E-Mailformaten S – SFX-Archive P – gepackte Objekte O – eingebettete OLE-Objekte
/EM:<"Masken">	Dateien nach Maske ausschließen Sie können mehrere Masken ausschließen, zum Beispiel EM:"*.txt;*.png; C\Videos*.avi".
/ET:<Anzahl der Sekunden>	Verarbeitung eines Objektes abbrechen, wenn sie mehr Sekunden dauert, als vom Wert <Anzahl der Sekunden> vorgegeben In der Grundeinstellung ist die Untersuchungsdauer nicht beschränkt.
/ES:<Größe>	Compound-Objekte von Untersuchung ausschließen, deren Größe den angegebenen Wert <Größe> in MB überschreitet In der Grundeinstellung untersucht Anti-Virus Objekte jeder Größe.
Zusätzliche Parameter (Options)	
/NOICHECKER	iChecker deaktivieren (standardmäßig aktiviert)
/NOISWIFT	iSwift deaktivieren (standardmäßig aktiviert)

Schlüssel	Beschreibung
/ALIAS:<Alias des Aufgabenamens>	Der Schlüssel vergibt an den Anti-Virus die Aufgabe zur Virensuche einen temporären Namen, mit dem die Aufgabe während ihrer Ausführung angesprochen werden kann, zum Beispiel, um die Statistik mit dem Befehl TASK anzuzeigen. Der Alias des Aufgabenamens muss unter den Aliases für die Aufgaben aller Funktionalkomponenten des Anti-Virus einmalig sein. Wenn dieser Schlüssel nicht vorgegeben ist, wird der alternative Name scan_<kavshell_pid> verwendet, beispielsweise scan_1234. Es wird dabei in der Anti-Virus-Konsole automatisch der Aufgabename Scan objects (<Datum und Uhrzeit>) vergeben, zum Beispiel: Scan objects 8/16/2007 5:13:14 PM.
Berichtsparameter (Report settings)	
/W:<Pfad zur Protokolldatei>	Wenn Sie diesen Schlüssel angeben, speichert Anti-Virus die Aufgabeereignisse in eine Datei, deren Pfad mit dem Schlüsselwert eingegeben wird. Protokolldatei enthält Statistik über Aufgabenausführung, Start- und Abschlusszeit der Aufgabe, und Informationen über Ereignisse. Im Bericht werden Ereignisse registriert, die in den Berichtsparametern und in den Parametern für das Ereignisjournal vorgegeben sind (Details finden Sie in Pkt. 13.2.7 auf S. 216). Sie können einen absoluten und einen relativen Pfad zur Protokolldatei eingeben. Wenn Sie nur den Namen der Berichtsdatei ohne einen Pfad angeben, wird die Datei im aktuellen Ordner angelegt. Ein neuerlicher Start des Befehls mit den gleichen Berichtsparametern überschreibt den vorhandenen Bericht mit dem gleichen Namen. Sie können die Protokolldatei während der Aufgabenausführung anzeigen. Der Aufgabenbericht wird im Knoten **Berichte** der Anti-Virus-Konsole dargestellt. Wenn Anti-Virus keine Berichtsdatei anlegen kann, unterbricht er die Befehlsausführung nicht und gibt keine Fehlermeldung aus.

16.4. Starten der Aufgabe *Vollständige Untersuchung des Computers*. KAVSHELL FULLSCAN

Verwenden Sie den Befehl KAVSHELL FULLSCAN, um die Systemaufgabe zur Virensuche **Vollständige Untersuchung des Computers** mit den Parametern zu starten, die in der Anti-Virus-Konsole der MMC vorgegeben sind.

Wenn Sie den Pfad in der Aufgabe zur Virensuche eingeben, können Sie Umgebungsvariablen verwenden. Verwenden Sie eine Umgebungsvariable, die für einen Benutzer bestimmt ist, geben Sie das Kommando KAVSHELL SCAN mit den Berechtigungen dieses Benutzers ein.

Syntax des Befehls KAVSHELL FULLSCAN

```
KAVSHELL FULLSCAN [/W:<Pfad zur Protokolldatei>]
```

Beispiele für den Befehl KAVSHELL FULLSCAN

`KAVSHELL FULLSCAN /W:fullscan.log` – Aufgabe zur Virensuche **Vollständige Untersuchung des Computers**ausführen; Bericht über Aufgabenereignisse in Datei fullscan.log im aktuellen Ordner speichern

Schlüssel	Beschreibung
/W:<Pfad zur Protokolldatei>	Wenn Sie diesen Schlüssel angeben, speichert Anti-Virus die Aufgabeereignisse in eine Datei, deren Pfad mit dem Schlüsselwert eingegeben wird. Protokolldatei enthält Statistik über Aufgabenausführung, Start- und Abschlusszeit der Aufgabe, und Informationen über Ereignisse. Im Bericht werden Ereignisse registriert, die in den Berichtsparametern und in den Parametern für das Ereignisjournal vorgegeben sind (Details finden Sie in Pkt. 13.2.7 auf S. 216). Sie können einen absoluten und einen relativen Pfad zur Protokolldatei eingeben. Wenn Sie nur den Namen der Berichtsdatei ohne einen Pfad angeben, wird die Datei im aktuellen Ordner angelegt. Ein neuerlicher Start des Befehls mit den gleichen Be-

Schlüssel	Beschreibung
	richtsparametern überschreibt den vorhandenen Bericht mit dem gleichen Namen. Sie können die Protokolldatei während der Aufgabenausführung anzeigen. Der Aufgabenbericht wird im Knoten **Berichte** der Anti-Virus-Konsole dargestellt. Wenn Anti-Virus keine Berichtsdatei anlegen kann, unterbricht er die Befehlsausführung nicht und gibt keine Fehlermeldung aus.

16.5. Asynchrone Aufgabenverwaltung. KAVSHELL TASK

Mit dem Befehl KAVSHELL TASK können Sie den angegebenen Aufgabe verwalten: Starten, Anhalten, Fortsetzen und Beenden einer Aufgabe sowie Anzeigen des aktuelles Status und einer Statistik. Der Befehl wird asynchron ausgeführt.

Syntax des Befehls KAVSHELL TASK

```
KAVSHELL TASK [<Alias des Aufgabenamens> </START | /STOP |
/PAUSE | /RESUME | /STATE | /STATISTICS >]
```

Beispiele für den Befehl KAVSHELL TASK

```
KAVSHELL TASK
KAVSHELL TASK on-access /START
KAVSHELL TASK user-task_1 /STOP
KAVSHELL TASK scan-computer /STATE
```

Schlüssel	Beschreibung
ohne Schlüssel	Der Befehl gibt eine Liste mit allen vorhandenen Aufgaben im Anti-Virus aus. Die Liste enthält die Felder: alternativer Name der Aufgabe, Aufgabenkategorie (Systemaufgabe, benutzerdefinierte Aufgabe oder Gruppenaufgabe) und den aktuellen Aufgabenstatus.

Schlüssel	Beschreibung
<Alias des Aufgaben-amens>	Statt eines Aufgabennamens verwenden Sie im Befehl SCAN TASK einen alternativen Namen (Task alias), ein zusätzlicher, kurzer Name, den Anti-Virus an Aufgaben vergibt. Um den Alias jedes Anti-Virus-Aufgaben anzuzeigen, geben Sie den Befehl KAVSHELL TASK ohne Schlüssel ein.
/START	Asynchrones Starten des angegebenen Aufgabe
/STOP	Beenden einer angegebenen Aufgabe
/PAUSE	Anhalten einer angegebenen Aufgabe
/RESUME	Asynchrones Fortsetzen einer angegebenen Aufgabe
/STATE	Aktuellen Aufgabenstatus abfragen (*Wird ausgeführt*, *Abgeschlossen*, *Angehalten*, *Beendet*, *Fehlerhaft abgeschlossen*, *Wird gestartet*, *Wird fortgesetzt*)
/STATISTICS	Aufgabenstatistik abfragen – Informationen über die Anzahl der Objekte, die seit dem Start der Aufgabe bis zum jetzigen Zeitpunkt verarbeitet wurden

16.6. Starten und Beenden der Aufgaben des Echtzeitschutzes. KAVSHELL RTP

Mit dem Befehl KAVSHELL RTP können Sie jede Aufgabe des Echtzeitschutzes starten oder beenden.

Syntax des Befehls KAVSHELL RTP

```
KAVSHELL RTP {/START | /STOP}
```

Beispiele für den Befehl KAVSHELL RTP

`KAVSHELL RTP /START` – Starten aller Aufgaben des Echtzeitschutzes

Schlüssel	Beschreibung
/START	Starten aller Aufgaben des Echtzeitschutzes

Schlüssel	Beschreibung
/STOP	Beenden aller Aufgaben des Echtzeitschutzes

16.7. Starten der Aufgabe zum Update der Anti-Virus-Datenbanken. KAVSHELL UPDATE

Mit dem Befehl KAVSHELL UPDATE können Sie die Aufgabe synchrones Update Anti-Virus-Datenbanken starten.

Aufgabe zum Update von Anti-Virus-Datenbanken, welche mithilfe des Befehls KAVSHELL UPDATE gestartet wird, ist zeitweilig. Sie wird in der MMC Anti-Virus-Konsole nur während der Ausführung angezeigt. Gleichzeitig wird ein Protokoll über Aufgabenausführung registriert; dieses wird im Knoten **Protokolle** der Anti-Virus-Konsole angezeigt. Für die Aufgaben zum Update, die mit dem Befehl KAVSHELL UPDATE angelegt und gestartet worden sind, wie für Aufgaben zum Update, die in der Anti-Virus-Konsole angelegt werden, werden die Richtlinien des Programms Kaspersky Administration Kit angewendet (Details zur Administration des Anti-Virus auf Servern mit dem Programm Kaspersky Administration Kit finden Sie in Kapitel 3 auf S. 43).

Wenn Sie den Pfad zur Update-Quelle eingeben, können Sie Umgebungsvariablen verwenden. Verwenden Sie eine Umgebungsvariable, die für einen Benutzer bestimmt ist, geben Sie das Kommando KAVSHELL UPDATE mit den Berechtigungen dieses Benutzers ein.

Syntax des Befehls KAVSHELL UPDATE

```
KAVSHELL UPDATE < Updatequelle | /AK | /KL> [/NOUSEKL]
[/PROXY:<Adresse>:<Port>] [/AUTHTYPE:<0-2>]
[/PROXYUSER:<Benutzername>] [/PROXYPWD:<Kennwort>]
[/NOPROXYFORKL] [/USEPROXYFORCUSTOM] [/USEPROXYFORLOCAL]
[/NOFTPPASSIVE] [/TIMEOUT:<Sekunden>] [/REG:<Code iso3166>]
[/W:<Name der Berichtsdatei>] [/ALIAS:<Alias des Aufgaben-
amens>]
```

Beispiele für den Befehl KAVSHELL UPDATE

`KAVSHELL UPDATE` – Starten der Benutzeraufgabe Update der Datenbanken

`KAVSHELL UPDATE \\Server\bases` – Starten der Aufgabe Update der Datenbanken, Update-Dateien werden im Netzwerkordner \\Server\bases gespeichert

`KAVSHELL UPDATE ftp://dnl-ru1.kaspersky-labs.com/ W:c:\update_report.log` – Starten der Aufgabe Update vom FTP-Server mit der Adresse ftp://dnl-ru1.kaspersky-labs.com/; Eintragen aller Aufgabeereignisse in die Protokolldatei c:\update_report.log.

`KAVSHELL UPDATE /KL  /PROXY:proxy.company.com:8080 /AUTHTYPE:1 /PROXYUSER:inetuser /PROXYPWD:123456` – Die Updates für die Anti-Virus-Datenbanken von dem Kaspersky-Lab-Updateserver herunterladen; Verbindung zur Updatequelle über Proxyserver aufbauen (Adresse des Proxyservers: proxy.company.com, Port: 8080); für den Zugriff auf den Server wird die in Microsoft Windows integrierte Authentifizierung (NTLM-authentication) unter dem Benutzerkonto (Benutzername: inetuser, Kennwort: 123456) verwendet.

Schlüssel	Beschreibung
Updatequelle (Pflichtschlüssel) Sie können eine oder mehrere Quellen angeben. Trennen Sie die Quellen mit Leerzeichen voneinander. <Pfad zur Updatequelle> Benutzerdefinierte Updatequelle.	
Pfad zum Netzwerkordner im UNC-Format. <URL>	Benutzerdefinierte Updatequelle – Pfad zum Netzwerkordner mit den Updates im UNC-Format (Universal Naming Convention).
<URL>	Benutzerdefinierte Updatequelle – Adresse des HTTP- oder FTP-Servers, auf dem sich der Update-Ordner befindet
<Lokaler Ordner>	Benutzerdefinierte Updatequelle – Ordner auf dem geschützten Server
/AK	Administrationsserver von Administration Kit als Updatequelle
/KL	Update-Server von Kaspersky Lab als Updatequelle
/NOUSEKL	Update-Service von Kaspersky Lab nicht verwenden, wenn andere Updatequellen nicht zur Verfügung stehen (als Standard werden sie verwendet)
Parameter des Proxyservers	

Schlüssel	Beschreibung
/PROXY:<Adresse>:< Port>	Netzwerkname oder IP-Adresse des Proxyservers und dessen Port. Wenn Sie diesen Schlüssel nicht angeben, verwendet Anti-Virus automatisch die Parameter des Proxyservers, der im lokalen Netzwerk verwendet wird.
/AUTHTYPE:<0-2>	Dieser Schlüssel bestimmt die Authentifizierung für den Zugang zum Proxyserver. In der Liste stehen die folgenden Werte: **0** – integrierte Microsoft Windows-Authentifizierung (NTLM-authentication); Anti-Virus geht mit dem Benutzerkonto **Lokales System** (**SYSTEM**) an den Proxyserver **1** – integrierte Microsoft Windows-Authentifizierung (NTLM-authentication); Anti-Virus geht mit dem Benutzerkonto an den Proxyserver, dessen Login und Kennwort mit den Schlüsseln /PROXYUSER und /PROXYPWD eingegeben werden **2** – Authentifizierung mit Login und Kennwort, die mit den Schlüsseln /PROXYUSER und /PROXYPWD (basic authentication) eingegeben werden Wenn für den Zugriff auf den Proxyserver keine Benutzerauthentifizierung benötigt wird, müssen Sie diesen Schlüssel nicht angeben.
/PROXYUSER:<Benutzername>	Name des Benutzers, der für den Zugang zum Proxyserver verwendet werden soll. Wenn Sie den Schlüsselwert /AUTHTYPE:0 angeben, werden die Schlüssel /PROXYUSER:<Benutzername> und /PROXYPWD:< Kennwort > ignoriert.
/PROXYPWD:<Kennwort>	Kennwort des Benutzers, der für den Zugang zum Proxyserver verwendet werden soll. Wenn Sie den Schlüsselwert /AUTHTYPE:0 angeben, werden die Schlüssel /PROXYUSER:<Benutzername> und /PROXYPWD:< Kennwort > ignoriert.. Wenn Sie den Schlüssel /PROXYUSER angeben und den Schlüssel /PROXYPWD auslassen, wird das Kennwort als leer aufgefasst.
/NOPROXYFORKL	Parameter des Proxyservers für Verbindung zu Update-Servern von Kaspersky Lab nicht verwenden (als Standard werden sie verwendet)

Schlüssel	Beschreibung
/USEPROXYFORCUSTOM	Parameter des Proxyservers für Verbindung zu benutzerdefinierten Updatequellen nicht verwenden (als Standard werden sie nicht verwendet)
/USEPROXYFORLOCAL	Parameter des Proxyservers für Verbindung zu benutzerdefinierten Servern verwenden. Wenn nichts angegeben ist, wird der Wert **Einstellungen des Proxyservers für Verbindung mit benutzerdefinierten Updatequellen nicht verwenden** übernommen. Details über die Parameter lesen Sie in Pkt. B.4.1 auf S. 413.
Allgemeine Parameter des FTP- und HTTP-Servers	
/NOFTPPASSIVE	Wenn Sie diesen Schlüssel angeben, verwendet Anti-Virus den FTP-Server im aktiven Modus für eine Verbindung zum geschützten Server. Wenn Sie diesen Schlüssel nicht angeben, verwendet Anti-Virus nach Möglichkeit den passiven Modus des FTP-Servers.
/TIMEOUT:<Anzahl der Sekunden>	Wartezeit für Verbindung mit FTP- oder HTTP-Server. Wenn Sie diesen Schlüssel nicht angeben, verwendet Anti-Virus den Standardwert: 10 Sek. Als Schlüsselwert können Sie nur ganze Zahlen eingeben.
/REG:<Code iso3166>	Der Schlüssel "Regionsoptionen" wird beim Update-Download von den Update-Servern bei Kaspersky Lab verwendet. Anti-Virus optimiert den Update-Download auf den geschützten Server, indem er den in der Nähe stehenden Update-Server ansteuert. Als Schlüsselwert geben Sie den alphabetischen Code des Landes an, in dem sich der geschützte Server befindet, entsprechend dem ISO-Standard 3166-1, zum Beispiel /REG:gr oder /REG:RU. Wenn Sie diesen Schlüssel auslassen oder einen nicht vorhandenen Ländercode eingeben, erkennt Anti-Virus den Standort des geschützten Servers je nach den Regionsoptionen des geschützten Servers (für Microsoft Windows 2003 Server und höher handelt sich um den Wert der Variable **Standort** (**Location**)).

Schlüssel	Beschreibung
/ALIAS:<Alias des Aufgabenamens>	Dieser Schlüssel weist einer Aufgabe einen temporären Namen zu, mit dem man die Aufgabe während seiner Ausführung ansprechen kann. Sie können beispielsweise die Aufgabenstatistik mit dem Befehl TASK anzeigen lassen. Der Alias des Aufgabenamens muss unter den Aliases für die Aufgaben aller Funktionalkomponenten des Anti-Virus einmalig sein. Wenn der Schlüssel nicht eingegeben ist, wird der Alias update_<kavshell_pid> verwendet, beispielsweise update_1234. In der Anti-Virus-Konsole wird an die Aufgabe der Name Anti-virus Update-bases (<date time>) vergeben, zum Beispiel Anti-virus Update-bases 8/16/2007 5:41:02 PM.
/W:<Pfad zur Protokolldatei>	Wenn Sie diesen Schlüssel angeben, speichert Anti-Virus die Aufgabeereignisse in eine Datei, deren Pfad mit dem Schlüsselwert eingegeben wird. Protokolldatei enthält Statistik über Aufgabenausführung, Start- und Abschlusszeit der Aufgabe, und Informationen über Ereignisse. Sie können einen absoluten und einen relativen Pfad zur Protokolldatei eingeben. Wenn Sie nur den Namen der Berichtsdatei ohne einen Pfad angeben, wird die Datei im aktuellen Ordner angelegt. Im Bericht werden Ereignisse registriert, die in den Berichtsparametern und in den Parametern für das Ereignisjournal vorgegeben sind (Details finden Sie in Pkt. 13.2.7 auf S. 216). Ein neuerlicher Start des Befehls mit den gleichen Berichtsparametern überschreibt den vorhandenen Bericht mit dem gleichen Namen. Sie können die Protokolldatei während der Aufgabenausführung anzeigen. Der Aufgabenbericht wird im Knoten **Berichte** der Anti-Virus-Konsole dargestellt. Wenn Anti-Virus keine Berichtsdatei anlegen kann, unterbricht er die Befehlsausführung nicht und gibt keine Fehlermeldung aus.

16.8. Rollback des Updates der Anti-Virus-Datenbanken. KAVSHELL ROLLBACK

Mit dem Befehl KAVSHELL ROLLBACK können Sie Systemaufgabe Rollback der Anti-Virus-Datenbanken bis zu den zuvor installierten Updates ausführen. Der Befehl wird synchron ausgeführt.

Syntax des Befehls

```
KAVSHELL ROLLBACK
```

16.9. Aktivierung und Deaktivierung von Schlüsseln. KAVSHELL LICENSE

Mit dem Befehl KAVSHELL LICENSE können Sie Lizenzschlüssel für den Anti-Virus installieren und löschen.

Syntax des Befehls KAVSHELL LICENSE

```
KAVSHELL LICENSE [/ADD: <Pfad zur Schlüsseldatei> [/R] |
/DEL: <Seriennummer>]
```

Beispiele für den Befehl KAVSHELL LICENSE

`KAVSHELL LICENSE /ADD: C:/License.key` – Schlüssel aus Datei installieren

`KAVSHELL LICENSE` – Informationen über installierte Schlüssel anzeigen;

`KAVSHELL LICENSE /DEL: 0000-000000-00000001` – installierten Schlüssel mit der Nummer 0000-000000-00000001 entfernen.

Schlüssel	Beschreibung
ohne Schlüssel	Der Befehl gibt die folgenden Informationen über die installierten Lizenzschlüssel aus: • Seriennummer des Schlüssels

Schlüssel	Beschreibung
	• Schlüsseltyp (für Beta-Tests, Demo-Schlüssel oder kommerziell) • Gültigkeitsdauer des Schlüssels • Vorhandensein eines Reserveschlüssels. Wenn der Wert * angegeben ist, ist der installierte Lizenz-schlüssel ein Reserveschlüssel.
/ADD: <Pfad zur Schlüsseldatei>	Es wird der Schlüssel aus der Datei mit dem Namen installiert, der mit dem Wert /ADD eingegeben wird. Fügen Sie den Dateinamen des Schlüssels und den kompletten Pfad an. Wenn Sie den Pfad zur Schlüsseldatei angeben, können Sie die Umgebungsvariablen des Systems verwenden. Dagegen können Sie die benutzerdefinierten Umgebungsvariablen nicht verwenden.
/R	Der Schlüssel /R ist ein Zusatz für den Schlüssel /ADD. Er weist darauf hin, dass der zu installierende Schlüssel ein Reserveschlüssel ist.
/DEL: {Seriennummer}	Löscht den Schlüssel mit der Seriennummer, die mit dem Wert /DEL eingegeben wird.

16.10. Erstellen des Protokolls der Ablaufverfolgung aktivieren, einstellen und deaktivieren. KAVSHELL TRACE

Mit dem Befehl KAVSHELL TRACE können Sie "on the fly" das Führen eines Protokolls zur Ablaufverfolgung aller Systeme des Anti-Virus aktivieren oder deaktivieren sowie die darin vorkommende Genauigkeitsstufe protokollieren lassen.

Syntax des Befehls KAVSHELL TRACE

```
KAVSHELL TRACE </ON /F:<Pfad zum Ordner der Logdateien>
[/S:<maximale Größe der Logdatei in Megabyte>]
[/LVL:debug|info|warning|error|critical] | /OFF>
```

Wenn das Protokoll der Ablaufverfolgung geführt wird und Sie dessen Parameter ändern wollen, geben Sie den Befehl KAVSHELL TRACE mit dem Schlüssel /ON sowie die Parameter für das Protokoll der Ablaufverfolgung mit den Schlüsselwerten /S und /LVL ein.

Schlüssel	Beschreibung
/ON	Führen des Protokolls der Ablaufverfolgung aktivieren
/F:<Ordner mit Dateien des Protokolls der Ablaufverfolgung>	Dieser Schlüssel gibt den vollständigen Pfad zum Ordner ein, in dem die Dateien mit dem Protokoll der Ablaufverfolgung (Pflichtschlüssel) gespeichert werden. Wenn Sie einen Pfad zu einem nicht vorhandenen Ordner eingeben, wird das Protokoll der Ablaufverfolgung nicht erstellt. Sie können die Netzwerkpfade im UNC-Format (Universal Naming Convention) angeben, können aber keine Pfade zu den Ordnern auf Netzwerk-Datenträgern des geschützten Servers eingeben. Wenn der Name einer eines Ordners, dessen Pfad Sie als Schlüsselwert eingeben, ein Leerzeichen enthält, schließen Sie den Pfad in Anführungszeichen ein, zum Beispiel: /F:"C\TRACE Folder". Wenn Sie den Pfad zu den Trace-Log-Dateien angeben, können Sie die Umgebungsvariablen des Systems verwenden. Dagegen können Sie die benutzerdefinierten Umgebungsvariablen nicht verwenden.
/S:<maximale Größe der Protokolldatei in Megabyte>	Dieser Schlüssel bestimmt die maximale Größe eines Protokolls der Ablaufverfolgung. Wenn die Größe der Protokolldatei den Höchstwert erreicht hat, beginnt Anti-Virus, Daten in eine neue Datei zu schreiben, die alte Protokolldatei wird gespeichert. Wenn Sie diesen Schlüssel nicht angeben, beträgt die maximale Größe einer Protokolldatei 50 MB.
/LVL:<debug | info | warning | error | critical>	Dieser Schlüssel bestimmt die Genauigkeitsstufe der Protokolldatei vom Maximum (*Debugging-Informationen*), bei dem alle Ereignisse im Log protokolliert werden, bis zum Minimum (*kritisch*), bei dem nur kritische Ereignisse erfasst werden. Wenn Sie diesen Schlüssel nicht angeben, werden in das Protokoll der Ablaufverfolgung Ereignisse mit der Genauigkeitsstufe *Debugging-Informationen* eingetragen.

Schlüssel	Beschreibung
/OFF	Dieser Schlüssel deaktiviert das Führen des Protokolls der Ablaufverfolgung.

Beispiele für den Befehl KAVSHELL TRACE:

KAVSHELL TRACE /ON /F:"C:\Trace Folder" /S:200 – Führen des Protokolls der Ablaufverfolgung mit der *Debugging-Informationen* und mit einer maximalen Größe der Protokolldatei von 200 MB aktivieren, Speichern der Datei im Ordner C:\Trace Folder.

KAVSHELL TRACE /ON /F:"C:\Trace Folder" /LVL:warning – Führen des Protokolls der Ablaufverfolgung mit der *Wichtige Ereignisse*; Speichern der Datei im Ordner C:\Trace Folder:

KAVSHELL TRACE /OFF – Führen des Protokolls der Ablaufverfolgung deaktivieren

16.11. Anlegen von Speicherauszugsdateien an- und ausschalten. KAVSHELL DUMP

Mit dem Befehl KAVSHELL DUMP können Sie "on the fly" das Erstellen von Speicherauszügen Anti-Virus-Prozesse bei anomalem Beenden aktivieren oder deaktivieren. Außerdem können Sie jederzeit Speicher-Images der vom Anti-Virus ausgeführten Prozesse abnehmen.

Syntax des Befehls KAVSHELL DUMP

```
KAVSHELL DUMP </ON /F:<Ordner mit Speicherauszugsdatei-
en>|/SNAPSHOT /F:<Ordner mit Speicherauszugsdateien> /
P:<pid> | /OFF>
```

Beispiele für den Befehl KAVSHELL DUMP:

KAVSHELL DUMP /ON /F:"C:\Dump Folder" – Erstellen des Speicherauszugs aktivieren, Speichern der Auszugsdatei im Ordner C:\Dump Folder

KAVSHELL DUMP /SNAPSHOT /F: C:\Dumps /P:1234 – Abnehmen eines Speicherauszugs vom Prozess mit der ID 1234 in den Ordner C:/Dumps

KAVSHELL DUMP /OFF – Erstellen des Auszugs deaktivieren

Schlüssel	Beschreibung
/ON	Aktivieren der Erstellung eines Speicherauszuges von einem Prozess bei dessen anomalem Beenden
{/F:<Pfad zum Ordner mit Auszugsdateien>}	Pflichtschlüssel, er gibt den Pfad zum Ordner an, in dem die Speicherauszugsdatei gespeichert wird. Wenn Sie einen Pfad zu einem nicht vorhandenen Ordner eingeben, wird die Speicherauszugsdatei nicht erstellt. Sie können die Netzwerkpfade im UNC-Format (Universal Naming Convention) verwenden, können aber keine Pfade zu den Ordnern auf Netzwerk-Datenträgern des geschützten Servers eingeben. Wenn Sie den Pfad zum Ordner mit den Speicherauszugsdateien angeben, können Sie die Umgebungsvariablen des Systems verwenden. Dagegen können Sie die benutzerdefinierten Umgebungsvariablen nicht verwenden.
/SNAPSHOT	Abnehmen eines Speicher-Images vom angegebenen Anti-Virus-Prozess und Speichern der Speicherauszugsdatei im Ordner, dessen Pfad der Schlüssel /F angibt.
/P	Prozess-PID-Nummer, die im Windows-Aufgabenmanager angezeigt wird
/OFF	Deaktivieren der Erstellung eines Speicherauszuges von Prozessen bei dessen anomalem Beenden

16.12. Import von Parametern. KAVSHELL IMPORT

Mit dem Befehl KAVSHELL IMPORT können Sie Anti-Virus-Parameter, Funktionen und Aufgaben aus einer Konfigurationsdatei in den Anti-Virus auf den geschützten Server importieren. Sie könne eine Konfigurationsdatei mit dem Befehl KAVSHELL EXPORT erstellen.

Syntax des Befehls KAVSHELL IMPORT

```
KAVSHELL IMPORT <Name der Konfigurationsdatei und Pfad>
```

Beispiele für den Befehl KAVSHELL IMPORT:

```
KAVSHELL IMPORT Server1.xml
```

Schlüssel	Beschreibung
<Name der Konfigurationsdatei und Pfad>	Name der Konfigurationsdatei, aus der die Parameter importiert werden. Wenn Sie den Pfad zur Datei angeben, können Sie die Umgebungsvariablen des Systems verwenden. Dagegen können Sie die benutzerdefinierten Umgebungsvariablen nicht verwenden.

16.13. Export von Parametern. KAVSHELL EXPORT

Mit dem Befehl KAVSHELL EXPORT können Sie alle Anti-Virus-Parameter und vorhandene Aufgaben in eine Konfigurationsdatei exportieren, um sie auf anderen Servern in den Anti-Virus zu importieren.

Syntax des Befehls KAVSHELL EXPORT

```
KAVSHELL EXPORT <Name der Konfigurationsdatei und Pfad>
```

Beispiele für den Befehl KAVSHELL EXPORT:

```
KAVSHELL EXPORT Server1.xml
```

Schlüssel	Beschreibung
<Name der Konfigurationsdatei und Pfad>	Name der Konfigurationsdatei, in der die Parameter gespeichert werden. Sie können an die Datei beliebige Erweiterung angeben. Wenn Sie den Pfad zur Datei angeben, können Sie die Umgebungsvariablen des Systems verwenden. Dagegen können Sie die benutzerdefinierten Umgebungsvariablen nicht verwenden.

KAPITEL 17. FEEDBACK-CODES

Die Feedback-Codes des Anti-Virus werden in allgemeine Codes unterteilt, die für alle Befehle der Befehlszeile gelten, und in Feedback-Codes für spezielle Befehle.

Feedback-Codes für die Befehle KAVSHELL SCAN и KAVSHELL FULLSCAN

Feedback-Code	Beschreibung
0	Vorgang erfolgreich ausgeführt (Es wurden keine Bedrohungen gefunden)
1	Vorgang abgebrochen
-2	Service nicht gestartet
-3	Zugriffsfehler
-4	Objekt nicht gefunden (Datei mit Liste der Untersuchungsbereiche nicht gefunden)
-5	Ungültige Befehlssyntax oder Untersuchungsbereich nicht festgelegt
-80	Es wurden infizierte Objekte gefunden
-81	Es wurden verdächtige Objekte gefunden
-82	Es wurden Verarbeitungsfehler erkannt
-83	Es wurden nicht untersuchte Objekte gefunden
-84	Es wurden beschädigte Objekte gefunden
-99	Unbekannter Fehler
-301	Ungültiger Schlüssel

Feedback-Codes für die Befehle KAVSHELL START und KAVSHELL STOP

Feedback-Code	Beschreibung
0	Vorgang erfolgreich ausgeführt

Feedback-Code	Beschreibung
-3	Zugriffsfehler
-5	Ungültige Befehlssyntax
-6	Ungültiger Vorgang (zum Beispiel ist der Anti-Virus-Service bereits gestartet oder schon beendet)
-7	Service ist nicht registriert
-8	Service-Start ist unterbunden
-9	Versuch des Service-Starts unter einem anderen Benutzerkonto war erfolglos (in Grundeinstellung arbeitet der Anti-Virus-Service mit dem Benutzerkonto **Lokales System**)
-99	Unbekannter Fehler

Feedback-Codes des Befehles KAVSHELL TASK

Feedback-Code	Beschreibung
0	Vorgang erfolgreich ausgeführt
-2	Service nicht gestartet
-3	Zugriffsfehler
-4	Objekt nicht gefunden (Aufgabe nicht gefunden)
-5	Ungültige Befehlssyntax
-6	Ungültiger Vorgang (zum Beispiel ist die Aufgabe nicht gestartet, schon gestartet oder kann nicht angehalten werden)
-99	Unbekannter Fehler
-301	Ungültiger Schlüssel
401	Aufgabe nicht gestartet (für Schlüssel /STATE)
402	Aufgabe ist schon gestartet (für Schlüssel /STATE)
403	Aufgabe ist schon angehalten (für Schlüssel /STATE)
-404	Fehler bei Vorgangsausführung (Ändern des Aufgabenstatus führte zum Absturz)

Feedback-Codes des Befehles KAVSHELL LICENSE

Feedback-Code	Beschreibung
0	Vorgang erfolgreich ausgeführt
-2	Service nicht gestartet
-3	Nicht ausreichende Rechte für Schlüsselverwaltung
-4	Objekt nicht gefunden (Schlüssel mit angegebener Seriennummer nicht gefunden)
-5	Ungültige Befehlssyntax
-6	Ungültiger Vorgang (Schlüssel ist schon installiert)
-99	Unbekannter Fehler
-301	Ungültiger Schlüssel
-303	Schlüssel ist für andere Anwendung

Feedback-Codes des Befehles KAVSHELL UPDATE

Feedback-Code	Beschreibung
0	Vorgang erfolgreich ausgeführt
200	Alle Objekte sind aktuell (Datenbanken oder Programm-Komponenten sind in einem aktuellen Zustand)
-2	Service nicht gestartet
-3	Zugriffsfehler
-5	Ungültige Befehlssyntax
-99	Unbekannter Fehler
-206	Updatedateien sind nicht vorhanden oder falsches Format
-209	Fehler bei Verbindung mit Updatequelle
-232	Anti-Virus hat Authentifizierungsprüfung beim Verbinden mit Proxyserver nicht bestanden
-234	Fehler bei Verbindung zum Programm Kaspersky Administration Kit

Feedback-Code	Beschreibung
-235	Anti-Virus hat die Authentifizierungsprüfung beim Verbinden mit Updatequelle nicht bestanden
-301	Ungültiger Schlüssel

Feedback-Codes des Befehles KAVSHELL ROLLBACK

Feedback-Code	Beschreibung
0	Vorgang erfolgreich ausgeführt
-2	Service nicht gestartet
-3	Zugriffsfehler
-99	Unbekannter Fehler
-221	Sicherungskopie der Datenbanken nicht gefunden
-222	Sicherungskopie der Datenbanken ist beschädigt

Feedback-Codes des Befehles KAVSHELL RTP

Feedback-Code	Beschreibung
0	Vorgang erfolgreich ausgeführt
-2	Service nicht gestartet
-3	Zugriffsfehler
-4	Objekt nicht gefunden (keine bzw. alle Aufgaben des Echtzeitschutzes nicht gefunden)
-5	Ungültige Befehlssyntax
-6	Ungültiger Vorgang (zum Beispiel Aufgabe ist schon gestartet oder schon beendet)
-99	Unbekannter Fehler
-301	Ungültiger Schlüssel

Feedback-Codes des Befehles KAVSHELL DUMP

Feedback-Code	Beschreibung
0	Vorgang erfolgreich ausgeführt
-2	Service nicht gestartet
-3	Zugriffsfehler
-4	Objekt nicht gefunden (keinen Pfad gefunden, der als Pfad zum Ordner mit den Auszugsdateien führt; keinen Prozess mit PID gefunden)
-5	Ungültige Befehlssyntax
-6	Ungültiger Vorgang (Versuch KAVSHELL DUMP /OFF auszuführen, wenn Erstellen der Speicherauszugsdateien deaktiviert ist)
-99	Unbekannter Fehler

Feedback-Codes des Befehles KAVSHELL TRACE

Feedback-Code	Beschreibung
0	Vorgang erfolgreich ausgeführt
-2	Service nicht gestartet
-3	Zugriffsfehler
-4	Objekt nicht gefunden (keinen Pfad gefunden, der als Pfad zum Ordner mit den Dateien für Protokoll der Ablaufverfolgung führt)
-5	Ungültige Befehlssyntax
-6	Ungültiger Vorgang (Versuch KAVSHELL TRACE /OFF auszuführen, wenn Erstellen des Protokolls der Ablaufverfolgung schon deaktiviert ist)
-99	Unbekannter Fehler

Feedback-Codes des Befehles KAVSHELL IMPORT

Feedback-Code	Beschreibung
0	Vorgang erfolgreich ausgeführt
-2	Service nicht gestartet
-3	Zugriffsfehler
-4	Objekt nicht gefunden (zu importierende Konfigurationsdatei nicht gefunden)
-5	Ungültige Syntax
-99	Unbekannter Fehler
501	Vorgang wurde erfolgreich ausgeführt, bei der Befehlsausführung ist jedoch ein Fehler / Hinweis aufgetreten, zum Beispiel hat Anti-Virus nicht die Parameter einer Funktionalkomponente importiert
-502	Zu importierende Datei ist nicht vorhanden oder hat ein unbekanntes Format
-503	Inkompatible Parameter (Konfigurationsdatei aus anderer Anwendung importiert oder Anti-Virus mit höherer Version oder inkompatibler Version)

Feedback-Codes des Befehles KAVSHELL EXPORT

Feedback-Code	Beschreibung
0	Vorgang erfolgreich ausgeführt
-2	Service nicht gestartet
-3	Zugriffsfehler
-5	Ungültige Syntax
-10	Konfigurationsdatei konnte nicht erstellt werden (z. B.; kein Zugang zum Ordner, welcher im Pfad vorgegeben wurde)
-99	Unbekannter Fehler

Feedback-Code	Beschreibung
501	Aktion erfolgreich abgeschlossen; Während der Ausführung des Befehls ist aber ein Fehler/Bemerkung aufgetreten, z.B. Anti-Virus konnte einige Parameter der funktionalen Komponente nicht exportieren.

TEIL 3. KONFIGURATION UND VERWALTUNG ÜBER KASPERSKY ADMINISTRATION KIT

Wenn in Ihren Unternehmen Kaspersky Administration Kit für die zentralisierte Verwaltung von Antiviren-Software benutzt wird, dann können Sie über die Administrationskonsole von Kaspersky Administration Kit die Antiviren-Software auf den geschützten Servern einstellen und verwalten.

In diesem Abschnitt stehen die folgenden Informationen:

- Verwaltung des Anti-Virus und Anzeige seines Status (s. Kapitel 18 auf S. 276)
- Erstellen und Einstellen von Richtlinien (s. Kapitel 19 auf S. 286)
- Einstellen des Anti-Virus im Dialogfenster **Einstellungen von Anwendung** (s. Kapitel 20 auf S. 300)
- Erstellen und Einstellen von Aufgaben (s. Kapitel 21 auf S. 333)

KAPITEL 18. ANTI-VIRUS VERWALTEN UND SEINEN STATUS ANZEIGEN

In diesem Kapitel stehen die folgenden Informationen:

18.1. Anti-Virus-Dienste starten und anhalten

Anti-Virus-Dienst wird beim Start von Betriebsystem automatisch gestartet. Dieser Dienst regelt die Arbeitsprozesse, welche die Aufgaben von ständigen Schutz, Scan nach Befehl und Update bedienen.

Standardmäßig werden beim Start des Anti-Virus-Dienst die Aufgaben **Echtzeitschutz für Dateien**, **Skript-Untersuchung, Untersuchung bei Systemstart** und **Integritätskontrolle anwenden** wie auch andere Aufgaben gestartet, die in dem Zeitplan den Eintrag der Starthäufigkeit **Bei Programmstart** zu stehen haben.

Wenn Sie den Anti-Virus-Dienst anhalten, wird das Ausführen aller Aufgaben angehalten. Nach dem Neustarten des Anti-Virus-Dienstes werden unterbrochene Aufgaben nicht automatisch neu gestartet. Es werden nur solche Aufgaben neu gestartet, die in dem Zeitplan die Starthäufigkeit **Beim Programmstart** zu stehen haben.

Um Anti-Virus-Dienst zu starten oder anzuhalten:

1. Öffnen Sie in der Struktur der Administrationskonsole den Knoten **Gruppen** und wählen Sie die Gruppe, zu der der geschützte Server gehört.

2. Öffnen Sie in der Ergebnisleiste das Kontextmenü auf der Zeile mit Informationen über den geschützten Server und wählen Sie den Befehl **Eigenschaften**.

3. Wählen Sie im Dialogfenster **Eigenschaften: <Computername>** auf der Registerkarte **Programme** in der Liste der installierten Anwendungen den Befehl **Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition** und klicken Sie auf die Schaltfläche **Eigenschaften**.

4. Öffnen Sie im Dialogfenster **Einstellungen der Anwendung** die Registerkarte **Allgemein**.

5. Führen Sie eine der Aktionen durch:

   - Um den Anti-Virus-Dienst zu starten, klicken Sie auf die Schaltfläche **Starten**.

   - Um den Anti-Virus-Dienst zu beenden, klicken Sie auf die Schaltfläche **Beenden**.

6. Klicken Sie auf **OK**.

18.2. Zustand des Serverschutzes anzeigen

In der Administrationskonsole können Sie den Zustand des Serverschutzes für einen ausgewählten Server anzeigen: Zustand der Aufgaben des **Echtzeitschutzes für Dateien** und der **Skript-Untersuchung**, den allgemeinen Status des Servers aus dem Blickwinkel der Antiviren-Sicherheit und seine Verfügbarkeit.

Um den Zustand des Schutzes für einen ausgewählten Server anzuzeigen, machen Sie Folgendes:

1. In der Administrationskonsole klappen Sie den Knoten **Gruppen** auf und gehen auf die Gruppe, zu der der geschützte Server gehört.

2. In dem Ergebnisfenster öffnen Sie das Kontextmenü mit einem Rechtsklick auf die Zeile mit dem geschützten Server und gehen Sie auf **Eigenschaften**.

3. Im Dialogfenster **Eigenschaften: <Name des Computers>** öffnen Sie die Registerkarte **Schutz** (s. Abbildung 93).

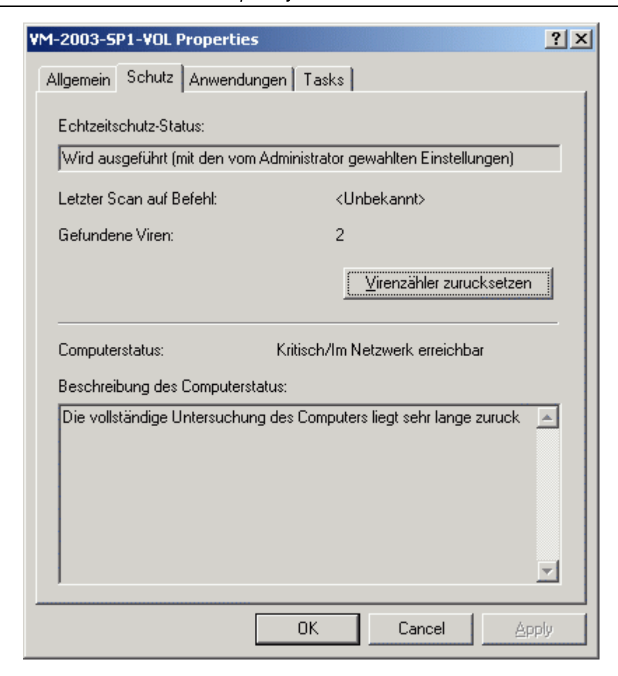


Abbildung 93. Dialogfenster **Eigenschaften: <Name des Computers>**, Registerkarte **Schutz**

Auf der Registerkarte **Schutz** sind die folgenden Informationen über den geschützten Server dargestellt:

Tabelle 23. Informationen über den geschützten Server auf der Registerkarte **Schutz**

Feld	Beschreibung
Echtzeitschutz-Status	Zeigt den Zustand der Aufgabe **Echtzeitschutz für Dateien: Wird ausgeführt** wenn Aufgaben **Echtzeitschutz für Dateien** oder **Skript-Untersuchung**. Wenn die Aufgabe **Echtzeitschutz für Dateien** ausgeführt wird, zeigt der Name den Status des Echtzeitschutzes der in der Aufgabe verwendeten Sicherheitsstufe: • **Empfohlen** – Sicherheitsparameter in der Aufgabe entsprechen der vordefinierten Stufe **Empfohlen** • **Maximaler Schutz** – Sicherheitsparameter entsprechen der vordefinierten Stufe **Maximale Sicherheit** • **Maximales Tempo** – Sicherheitsparameter entsprechen der vordefinierten Stufe **Maximales Tempo** • **Benutzerdefinierte Einstellungen** - Sicherheitsparameter entsprechen der vordefinierten Sicherheitsstufe **Anderer** Details über die vordefinierten Sicherheitsstufen finden Sie in Pkt. 6.2.2.1 auf S. 79.
Letzte Virensuche	Datum und Uhrzeit für die Ausführung einer Aufgabe des letzten Scans auf Befehl mit dem Status "Aufgabe Vollständige Untersuchung des Computers".
Gefundene Viren	Gesamtzahl der schädlichen Programme (Namen der Bedrohungen), die auf dem geschützten Server gefunden wurden (Zähler für gefundene Bedrohungen) seit dem Installieren des Antivirendienstes oder seit dem der Virenzähler zurück gesetzt wurde. Um den Virenzähler zurück zu setzen, klicken Sie auf die Schaltfläche **Virenzähler zurücksetzen**.
Beschreibung des Computerstatus	Serverstatus aus der Sicht des Antivirenschutzes. Details über Computerstatus lesen Sie auf der Seite des technischen Dienstes von "Kaspersky Lab", Artikelnummer: **987**.

18.3. Anti-Virus-Statistik anzeigen

In der Administrationskonsole können Sie statistische Informationen über Anti-Virus auf dem jeweiligen Server anzeigen: Anzahl der Prozesse des Anti-Virus, Anzahl der Einträge in den installierten Anti-Virus-Datenbanken, Erstellungsdatum der zuletzt installierten Anti-Virus-Datenbanken sowie Informationen über die Funktionen der einzelnen Anti-Virus-Komponenten und Aufgabenausführung.

> **Anmerkung**
>
> Wenn Sie die Statistik in Echtzeit verfolgen wollen, öffnen Sie den Port UDP 15000 im Windows-Firewall des Computers, an dem der Administrationsserver installiert ist.

Um die Anti-Virus-Statistik anzuzeigen, machen Sie Folgendes:

1. In der Administrationskonsole klappen Sie den Knoten **Gruppen** auf und gehen auf die Gruppe, zu der der geschützte Server gehört.

2. In dem Ergebnisfenster öffnen Sie das Kontextmenü mit einem Rechtsklick auf die Zeile mit dem geschützten Server und gehen Sie auf **Eigenschaften**.

3. Im Dialogfenster **Computerparameter (Properties)** gehen Sie auf der Registerkarte **Anwendungen Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition** in die Liste der installierten Anti-Virus-Anwendungen und klicken auf die Schaltfläche **Statistik**. Es öffnet sich das Dialogfenster **Statistik** (s. Abbildung 94).



Abbildung 94. Dialogfenster **Statistik**

Im Dialogfenster **Statistik** werden die folgenden Informationen angezeigt:

Tabelle 24. Informationen über den Zustand des Anti-Virus auf dem geschützten Server

Feld	Beschreibung
Erstellungsdatum der Datenbanken (UTC)	Datum und Uhrzeit der Veröffentlichung der Datenbanken durch Kaspersky Lab, im Format (Coordinated Universal Time)
Anzahl der aktiven Prozesse	Anzahl der Arbeitsprozesse des Anti-Virus, die die Aufgaben des Echtzeitschutzes, Virensuche und Update momentan durchführen
Anzahl der Einträge in den Datenbanken	Allgemeine Anzahl der Einträge in den auf dem Server installierten Anti-Virus-Datenbanken
Statistik für Quarantäne	Informationen über aktuellen Zustand der Quarantäne
Statistik für Echtzeitschutz	Informationen über die Aufgabe **Echtzeitschutz für Dateien** (Details finden Sie in Pkt. 6.3 auf S. 91)

Statistik für Sperrungen	Informationen über Anzahl der Rechner, deren Zugriff auf den geschützten Server seit dem letzten Start des Anti-Virus gesperrt worden ist (Details finden Sie in Pkt. 7.9 auf S. 107)
Statistik für Virensuche	Informationen über laufende Aufgaben zur Virensuche (Details finden Sie in Pkt. 9.4 auf S. 146)
Statistik für Skript-Untersuchung	Informationen über die Anzahl der Skripte, die Anti-Virus seit dem Start der Aufgabe **Skript-Untersuchung** bearbeitet hat (Details finden Sie in Pkt. 6.5 auf S. 95)
Statistik für Backup	Informationen über den aktuellen Zustand des Backup (Details finden Sie in Pkt. 12.6 auf S. 201)

Anmerkung

Informationen über die Aufgabe **Echtzeitschutz für Dateien**, **Skript-Untersuchung** und über Aufgaben zur Virensuche werden nur dann angezeigt, wenn die entsprechende Aufgabe ausgeführt wird.

18.4. Informationen über Anti-Virus anzeigen

Sie können Information über Anti-Virus und seine Datenbanken ansehen.

Um Informationen über Anti-Virus anzuzeigen:

1. Öffnen Sie in der Struktur der Administrationskonsole den Knoten **Gruppen** und wählen Sie die Gruppe, zu der der geschützte Server gehört.
2. Öffnen Sie in der Ergebnisleiste das Kontextmenü auf der Zeile mit Informationen über den geschützten Server und wählen Sie den Befehl **Eigenschaften**.
3. Wählen Sie im Dialogfenster **Eigenschaften: <Computername>** auf der Registerkarte **Programme** in der Liste der installierten Anwendungen den Befehl **Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition** und klicken Sie auf die Schaltfläche **Eigenschaften**.

4. Öffnen Sie im Dialogfenster **Einstellungen der Anwendung** die Registerkarte **Allgemein**.

Auf der Registerkarte **Allgemein** (s. Abbildung 103) werden dargestellt:

- Allgemeine Informationen über Anti-Virus:
    - Versionsnummer
    - Installationsdatum und Uhrzeit
    - Datum und Uhrzeit des letzten Updates für Anti-Virus-Module
    - Zustand des Anti-Virus-Dienstes (gestartet/beendet)
- Informationen über Datenbanken des Anti-Virus
    - Datum und Uhrzeit der Erstellung der installierten Updates (in dem Format, das den Regionsoptionen des Computers entspricht, auf dem die Administrationskonsole installiert ist)
    - Allgemeine Anzahl der Einträge in den Datenbanken
    - Datum und Uhrzeit des letzten Updates

18.5. Informationen über installierte Schlüssel anzeigen

Um Informationen über installierte Lizenzschlüssel anzuzeigen:

1. Öffnen Sie in der Struktur der Administrationskonsole den Knoten **Gruppen** und wählen Sie die Gruppe, zu der der geschützte Server gehört.
2. Öffnen Sie in der Ergebnisleiste das Kontextmenü auf der Zeile mit Informationen über den geschützten Server und wählen Sie den Befehl **Eigenschaften**.
3. Wählen Sie im Dialogfenster **Eigenschaften: <Computername>** auf der Registerkarte **Programme** in der Liste der installierten Anwendungen den Befehl **Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition** und klicken Sie auf die Schaltfläche **Eigenschaften**.
4. Öffnen Sie im Dialogfenster **Einstellungen von Anwendung** die Registerkarte **Lizenzen** (s. Abbildung 95).

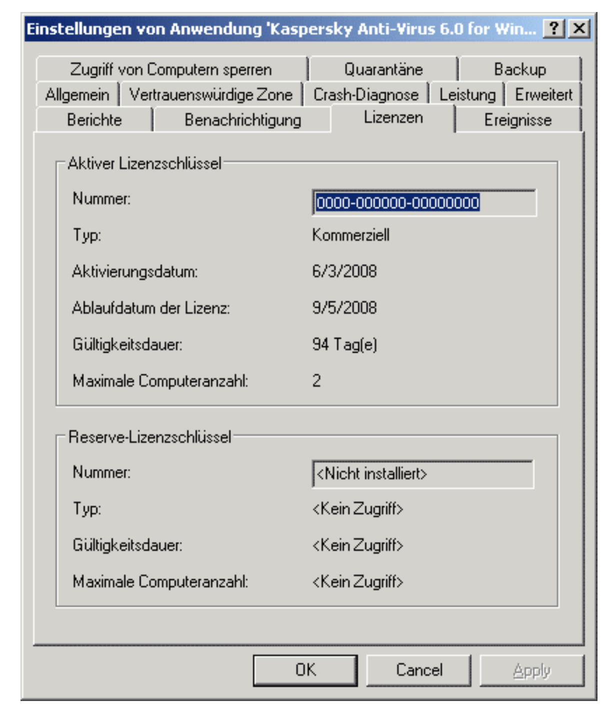


Abbildung 95. Dialogfenster **Einstellungen von Anwendung**, Registerkarte **Lizenzen**

Auf der Registerkarte **Lizenzen** werden die folgenden Informationen über installierte Lizenzschlüssel angezeigt:

Tabelle 25. Informationen über installierte Lizenzschlüssel

Feld	**Beschreibung**
Nummer	Seriennummer des Schlüssels
Typ	Schlüsseltyp: (Für Beta-Test, Demo-Schlüssel, kommerzieller Schlüssel). Details über Schlüsseltyp lesen Sie in Pkt. 14.1 auf S. 229.
Aktivierungsdatum	Installationsdatum des Schlüssels (nur für aktiven Schlüssel)
Ablaufdatum der Lizenz	Ablaufdatum für die Gültigkeit des Lizenzschlüssels (nur für aktiven Schlüssel); Anti-Virus errechnet diesen Termin bei der Installation des Schlüssels, er tritt ein, wenn die *Funktionsperiode* des Lizenz-

Feld	Beschreibung
	schlüssels seit seiner Aktivierung verstrichen ist, er liegt aber nicht nach dem *Termin, an dem der Schlüssel ungültig wird*
Gültigkeitsdauer	Anzahl der Tage bis zum Ablauf der Gültigkeits-dauer des Schlüssels
Maximale Computeran-zahl	Im Schlüssel vorgesehenen Begrenzung (wenn vor-handen)

KAPITEL 19. RICHTLINIEN ERSTELLEN UND VERWALTEN

In diesem Kapitel stehen die folgenden Informationen:

19.1. Richtlinien

Sie können einheitliche Richtlinien in Kaspersky Administration Kit Richtlinien erstellen, um den Schutz auf mehreren Server zu verwalten, auf denen Anti-Virus installiert ist.

Eine *Richtlinie* übernimmt die in ihr eingetragenen Parameterwerte des Anti-Virus, seine Funktionen und Aufgaben auf allen geschützten Servern einer Administrationsgruppe.

> **Anmerkung**
>
> Mit Richtlinien können Sie keine Schutzbereiche (Untersuchungsbereiche) in den Aufgaben **Echtzeitschutz für Dateien** und **Virensuche** erstellen.

Sie können mehrere Richtlinien für eine Administrationsgruppe erstellen und sie temporär übernehmen. In der Administrationskonsole hat eine Richtlinie, die zurzeit in der Gruppe gilt, den Status *aktiv*.

Informationen über den Geltungsbereich einer Richtlinie werden im Bericht zum System-Audit des Anti-Virus registriert. Sie können eine Richtlinie in der Anti-Virus-Konsole in der MMC im Knoten **Bericht zum System-Audit** anzeigen.

Aus den Geltungsarten von Richtlinien können Sie nur die Methode **Parameter nicht ändern** zulässig, bei der die in der Richtlinie festgelegten Parameter im Anti-Virus gespeichert werden. Sie können die Geltungsarten für Richtlinien **Pflicht-Parameter ändern** und **Alle Parameter ändern** nicht einsetzen.

Entsprechend der Geltungsart für Richtlinien **Parameter nicht ändern** übernimmt Anti-Virus während der Geltung die Parameterwerte, neben denen Sie in den Richtlinieneigenschaften das Symbol 🔒 gesetzt haben, statt die Parameterwerte heranzuziehen, die bis zur Übernahme der Richtlinie gegolten haben. Anti-Virus übernimmt keine Parameterwerte, neben denen in den Richtlinieneigenschaften das Zeichen 🔓 gesetzt ist. Sobald die Gültigkeitsdauer einer Richtlinie endet, werden die Parameter, deren Werte durch die Richtlinie geändert wurden, erneut auf die Werte zurückgesetzt, die vor dem Übernehmen der Richtlinie galten.

Während der Richtliniengeltung werden in der Anti-Virus-Konsole in der MMC und im Dialogfenster **Einstellungen von Anwendung** der Administrationskonsole Parameterwerte angezeigt, die in der Richtlinie mit dem Symbol 🔒 gekennzeichnet sind. Sie lassen sich nicht bearbeiten. Die Werte der anderen Parameter (die in der Richtlinie mit dem Symbol 🔓 gekennzeichnet sind) lassen sich in der Anti-Virus-Konsole in der MMC im Dialogfenster **Einstellungen von Anwendung** der Administrationskonsole bearbeiten.

Wenn eine Richtlinie Parameter für eine der Aufgaben des Echtzeitschutzes bestimmt und die Aufgabe ausgeführt wird, dann werden diese Parameter sofort übernommen, wenn die Richtlinie aktiv wird. Wenn die Aufgabe nicht ausgeführt wird, werden die Parameter aus der Richtlinie beim nächsten Aufgabenstart übernommen. Wenn durch die Richtlinie die Parameter anderer Anti-Virus-Aufgaben bestimmt werden, dann werden, wenn die Richtlinie aktiv wird, diese Parameter nicht für die ausgeführten Aufgaben übernommen, sondern beim nächsten Aufgabenstart.

19.2. Richtlinie erstellen

Das Erstellen einer Richtlinie besteht aus zwei Etappen:

1. Mit dem Assistenten für die Erstellung von Richtlinien erstellen Sie eine Richtlinie. In den Fenstern des Assistenten können Sie die Parameter der Aufgaben **Update der Datenbanken**, **Update der Programm-Module**, **Echtzeitschutz für Dateien** und **Virensuche** aktivieren.

2. Im Dialogfenster **Richtlinieneigenschaften** aktivieren Sie je nach Ihren Wünschen die Parameter für die übrigen Aufgaben und Anti-Virus-Parameter.

   Im Dialogfenster **Richtlinieneigenschaften** können Sie die mit dem Assistenten für die Erstellung von Richtlinien eingestellten Parameter für Aufgaben zum Update und für Aufgaben zur Virensuche sowie für die Aufgabe **Echtzeitschutz für Dateien** ändern. Details dazu, wie eine angelegte Richtlinie eingestellt wird, finden Sie in Pkt. 19.3 auf S. 293.

Um eine Richtlinie für eine Anti-Virus-Servergruppe zu erstellen:

1. In der Administrationskonsole klappen Sie den Knoten **Gruppen** auf, danach klappen Sie die Administrationsgruppe auf, für deren Server Sie eine Richtlinie erstellen werden.

2. Aus dem Kontextmenü des eingebetteten Knotens **Richtlinien** gehen Sie auf den Eintrag **Neu** → **Richtlinie.**

   Darauf öffnet sich Richtlinien-Assistent.

3. Im Fenster **Name der Richtlinie** tragen Sie im Eingabefeld den Namen der zu erstellenden Richtlinie ein. (Name darf die Zeichen **" * < : > ? \ / |** nicht enthalten).

4. Im Fenster **Anwendung** klicken Sie unter dem Kopf **Anwendung** auf **Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition**.

5. Im Fenster **Neue Gruppenrichtlinie für die Anwendung erstellen** wählen Sie einen der folgenden Zustände für die Richtlinie aus:

   - **Aktive Richtlinie**, wenn Sie möchten, dass die Richtlinie sofort nach dem Erstellen in Kraft tritt. Wenn in der Gruppe bereits eine aktive Richtlinie existiert, dann wird diese existierende Richtlinie außer Kraft treten, und die neu erstellte wird zur aktiven Richtlinie.

   - **Inaktive Richtlinie**, wenn Sie nicht möchten, dass die Richtlinie sofort angewendet wird. Sie können die Richtlinie später aktivieren.

   In den darauf folgenden Fenster des Richtlinien-Assistenten setzen Sie folgende Parameter entsprechend Ihren Bedürfnissen ein: **Update der Datenbanken**, **Update der Programm-Module**, **Echtzeitschutz für Dateien** und **Virensuche**.

6. Im Fenster **Echtzeitschutz für Dateien** (s. Abbildung 96) wählen Sie den Schutzmodus für Objekte in der Aufgabe **Echtzeitschutz für Dateien** und wählen Sie eine der vordefinierten Sicherheitsstufen aus oder konfigurieren Sie manuell die Parameter für Sicherheit (s. Pkt. B.3 auf S. 395).

   Aktivieren Sie das Kontrollkästchen **Vertrauenswürdige Zone anwenden**, wenn Sie in der Aufgabe **Echtzeitschutz für Dateien** vom Schutzbereich diejenigen Objekte ausschließen wollen, die in der vertrauenswürdigen Zone des Anti-Virus beschrieben werden (Details zur vertrauenswürdigen Zone lesen Sie in Pkt. 8.1 auf S. 109; wie Ausnahmen in die vertrauenswürdige Zone im Programm Kaspersky Administration Kit aufgenommen werden, lesen Sie in Pkt. 20.7 auf S. 323).

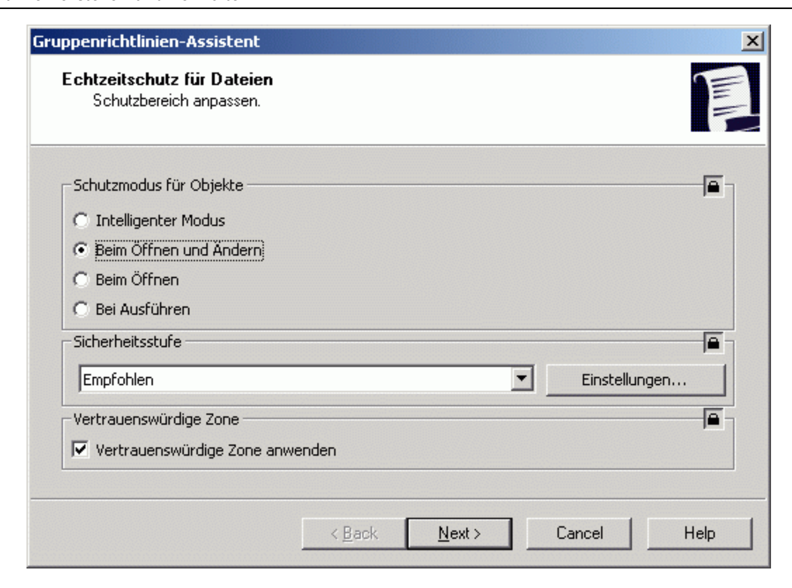


Abbildung 96. Fenster **Echtzeitschutz für Dateien**

7. Im Fenster **Virensuche** (s. Abbildung 97) wählen Sie einer der vordefinierten Sicherheitsstufen aus oder konfigurieren Sie manuell die Parameter für Sicherheit in den Aufgabe zur Virensuche ein (s. Pkt. B.3 auf S. 395).

   Aktivieren Sie das Kontrollkästchen **Vertrauenswürdige Zone anwenden**, wenn Sie in der Aufgabe zur Virensuche vom Schutzbereich diejenigen Objekte ausschließen wollen, die in der vertrauenswürdigen Zone des Anti-Virus beschrieben werden (Details zur vertrauenswürdigen Zone lesen Sie in Pkt. 8.1 auf S. 109; wie Ausnahmen in die vertrauenswürdige Zone im Programm Kaspersky Administration Kit aufgenommen werden, lesen Sie in Pkt. 20.7 auf S. 323).

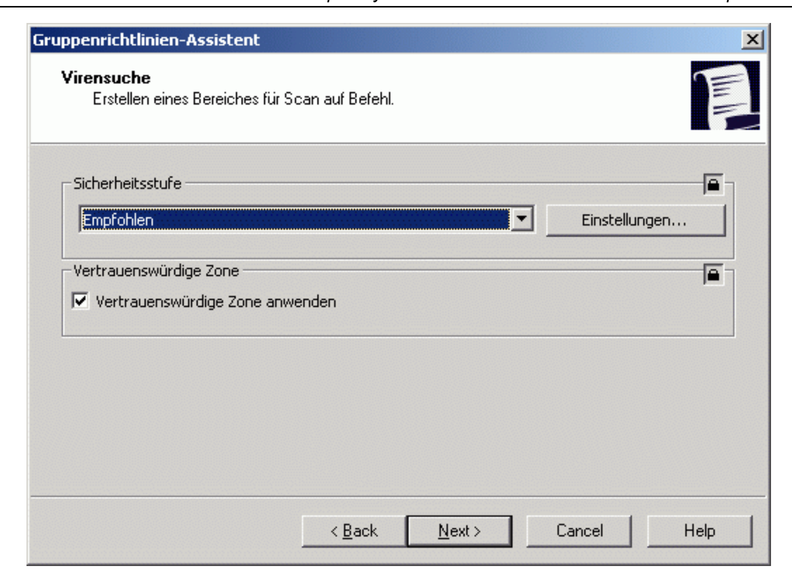


Abbildung 97. Fenster **Virensuche**

8. Im Fenster **Update** (s. Abbildung 98) stellen Sie die Parameter für die Aufgaben **Update der Datenbanken** und **Update der Programm-Module** ein.

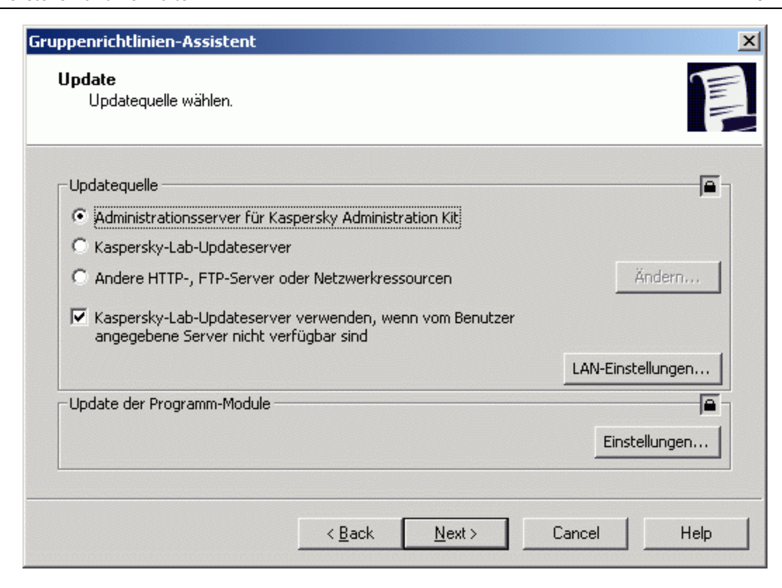


Abbildung 98. Fenster **Update**

9. Im Fenster **Einstellungen** führen Sie folgende Aktionen durch:

   a) Wählen Sie eine Updatequelle aus (s. Pkt. B.5.1 auf S. 419).

   b) Klicken Sie auf die Schaltfläche **LAN-Einstellungen**. Im Dialogfenster **Verbindungseinstellungen** stellen Sie die gewünschten Parameter für die Verbindung ein:

      - Ändern Sie die Einstellungen das FTP-Servers für die Verbindung mit dem geschützten Server und das Zeitlimit bei der Verbindungsaufnahme (s. Pkt. B.5.2 auf S. 421).

      - Stellen Sie die Zugangsparameter für den Proxy-Server während der Verbindung mit der Updatequelle ein (s. Pkt. B.5.4 auf S. 422).

      - Auf Registerkarte **Regionsoptionen** wählen Sie die Lage des geschützten Servers (der Server) aus, um den Update-Download zu optimieren (s. Pkt. B.5.5 auf S. 425).

   c) Um die Parameter der Aufgabe **Update der Programm-Module** einzustellen, klicken Sie im Fenster **Update** auf die Schaltfläche **Einstellungen** unter dem Kopf **Update der Programm-Module** und stellen Sie im Dialogfenster **Einstellungen des Updates für Programm-Module** (s. Abbildung 69) die Update-Parameter für die Programm-Module ein:

- Wählen Sie aus, ob Updates der Programm-Module geladen und installiert werden sollen oder ob nur das Vorhandensein von Updates überprüft werden soll. (s. Pkt. B.5.6.1 auf S. 426)

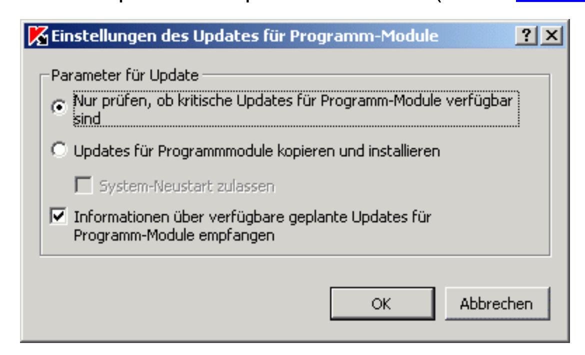


Abbildung 99. Dialogfenster **Einstellungen des Updates für Programm-Module**

- Damit Anti-Virus nach dem Abschluss der Aufgabe den Server automatisch neu startet, wenn der Neustart zum Übernehmen von installierten Programm-Modulen erforderlich ist, aktivieren Sie das Kontrollkästchen **System-Neustart zulassen**.

- Wenn Sie Daten über die Veröffentlichung von geplanten Updates für Anti-Virus-Module downloaden wollen, setzen Sie das Häkchen im Kontrollkästchen **Informationen über verfügbare geplante Updates für Programm-Module empfangen**.

  Kaspersky Lab veröffentlicht geplante Update-Pakete nicht auf den Updateservern zum automatischen Updaten, sondern Sie laden sich solche Updates von der Kaspersky-Lab-Internetseite. Sie können einstellen, den Administrator über das Ereignis **Geplante Update für Anti-Virus-Module sind verfügbar** zu benachrichtigen, so dass er die Adresse unserer Internetseite erfährt, von der Sie die geplanten Updates downloaden können (Details zur Einstellung von Benachrichtigungen finden Sie in Pkt. 15.2 auf S. 237).

> **Anmerkung**
>
> Die Parameter für die Aufgabe **Update-Verteilung** können Sie später im Dialogfenster **Eigenschaften: <Richtlinie>** einstellen.

10. Im Fenster **Beenden** klicken Sie auf die Schaltfläche **Fertig**.

Die erstellte Richtlinie wird in der Richtlinienliste im Knoten **Richtlinien** der ausgewählten Administrationsgruppe angezeigt. Jetzt können Sie im

Dialogfenster **Eigenschaften: <Richtlinie>** andere Anti-Virus-Parameter, Funktionen und Aufgaben einstellen.

19.3. Richtlinie einstellen

Im Dialogfenster **Eigenschaften** einer vorhandenen Richtlinie können Sie die allgemeine Anti-Virus-Parameter, Parameter der Funktionen und Aufgaben für Server einstellen, die zu einer Administrationsgruppe gehören.

Anmerkung

Mit Richtlinien können Sie keine Schutzbereiche (Untersuchungsbereiche) in der Aufgabe **Echtzeitschutz für Dateien** und in den Aufgaben zur Virensuche erstellen.

Um die Parameter im Dialogfenster ***Eigenschaften: <Richtlinie>*** *einzustellen, machen Sie Folgendes:*

1. In der Administrationskonsole klappen Sie den Knoten **Gruppen** auf, klappen Sie die Administrationsgruppe auf, für die Sie die Richtlinienparameter einstellen wollen, danach klappen Sie den eingebetteten Knoten **Richtlinien** auf.
2. Im Ergebnisfenster öffnen Sie das Kontextmenü mit einem Rechtsklick auf die Richtlinie, deren Parameter Sie einstellen wollen, und gehen Sie auf **Eigenschaften**.
3. Im Dialogfenster **Eigenschaften: <Richtlinie>** (s. Abbildung 100) stellen Sie die gewünschten Richtlinienparameter ein.

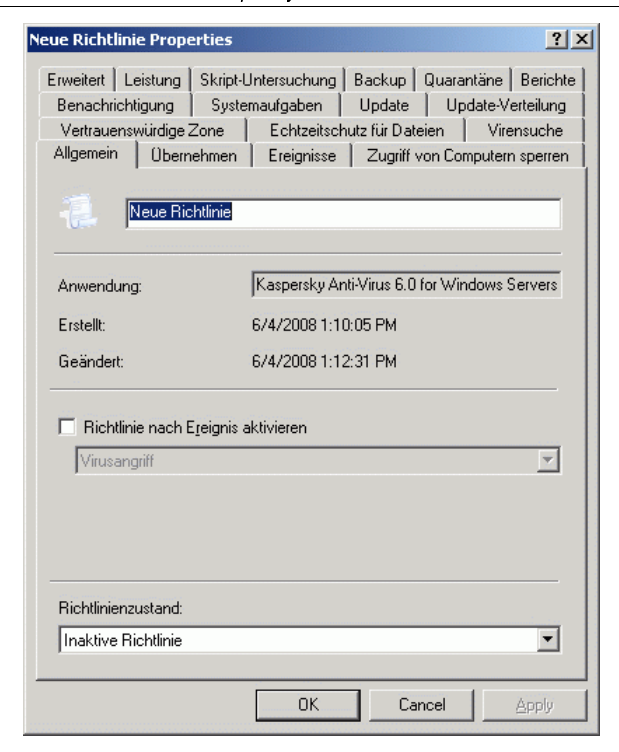


Abbildung 100. Beispiel für das Dialogfenster **Eigenschaften: <Richtlinie>**

Sie können die Richtlinienparameter auf folgenden Registerkarten einstellen:

Tabelle 26. Richtlinienparameter

Parameter	**Registerkarte**
Sicherheitsparameter in der Aufgabe **Echtzeitschutz für Dateien**: • **Schutzmodus für Objekte** (Beschreibung der Parameter s. Pkt. B.3.1 auf S. 396); • **Sicherheitsstufe** (einheitliche Parameter für den gesamten Schutzbereich): Sie können eine vordefinierte Sicherheitsstufe wählen (Beschreibung s. Pkt. 6.2.2.1 auf S. 79) oder die Sicherheitsparameter manuell anpassen (genauso wie in der	**Echtzeitschutz für Dateien**

Parameter	Registerkarte
MMC-Konsole - siehe Anleitung auf S. 82).;	
• Parameter für das automatische Sperren des Zugriffs von Computern (siehe Anleitung auf S. 306); • Ausschließen von Computern aus der Sperre (Vertrauenswürdige Computer) (siehe Anleitung auf S. 309); • Verhinderung von Virus-Epidemien (siehe Anleitung auf S. 310)	**Zugriff von Computern sperren**
• Erlaubnis oder Verbot der Ausführung von verdächtigen Skripts (Details über den Parameter lesen Sie in Pkt. 6.1 auf S. 68). • Verwendung er vertrauenswürdigen Zone – Kapitel 8 auf S. 109).	**Skript-Untersuchung**
• Liste der vertrauten Prozesse verwalten (gleich, wie im Fenster **Einstellungen von Anwendung** s. Pkt. 20.7.1 auf S. 324); • Echtzeitschutz für die Dateien abschalten, welche während des Backups kopiert werden (gleich, wie im Fenster **Einstellungen von Anwendung** s. Pkt. 20.7.2 auf S. 326) • Anlegen und Übernehmen von Ausnahmen der vertrauenswürdigen Zone (s. Pkt. 20.7 auf S. 323).	**Vertrauenswürdige Zone**
Sicherheitsparameter für Aufgaben zur Virensuche (gleich für alle Schutzbereiche): Sie können eine vordefinierte Stufe wählen (s. Beschreibung in Pkt. 9.2.2.1 auf S. 132) oder Sicherheitsparameter manuell konfigurieren (gleich, wie in der MMC-Konsole – s. Anleitung auf S. 135).	**Virensuche**

Parameter	Registerkarte
Parameter für die Aufgaben zum Update **Update der Datenbanken** und **Update der Programm-Module** • Updatequelle auswählen (Details über Parameter lesen Sie in Pkt. B.5.1 auf S. 419); • Verbindungsparameter mit der Update-quelle einstellen und Region des ge-schützten Server angeben, um Update zu optimieren (Schaltfläche **LAN-Einstellungen**) (gleich, wie in der MMC-Konsole – s. Anleitung auf S. 159); • **Update der Programm-Module** einstel-len (Schaltfläche **Einstellungen**) (gleich, wie in der MMC-Konsole – s. Anleitung auf S. 164).	**Update**
Parameter der Aufgabe **Update-Verteilung** • Updatequelle auswählen (Details über Parameter lesen Sie in Pkt. B.5.1 auf S. 419); • Verbindungsparameter mit der Update-quelle einstellen und Region des ge-schützten Server angeben, um Update zu optimieren (Schaltfläche **LAN-Einstellungen**) (gleich, wie in der MMC-Konsole – s. Anleitung auf S. 159); • Parameter der Aufgabe **Update-Verteilung** einstellen (gleich, wie in der MMC-Konsole – s. Anleitung auf S. 166).	**Update-Verteilung**
Zeitplan für Systemaufgaben abschalten (s. Pkt. 19.4 auf S. 297)	**Systemaufgaben**
Quarantäne-Parameter (gleich, wie im Fens-ter **Einstellungen von Anwendung** s. An-leitung auf S. 316)	**Quarantäne**
Backup-Parameter (gleich, wie im Fenster **Einstellungen von Anwendung** s. Anlei-tung auf S. 319)	**Backup**

Parameter	Registerkarte
Allgemeine Anti-Virus-Parameter	**Leistung** und **Erweitert**
Benachrichtigungen für Administrator und Benutzer über die Anti-Virusereignisse einstellen	**Benachrichtigungen**
Berichte einstellen	**Berichte**
Benachrichtigungen für Administrator und Benutzer über die Anti-Virusereignisse einstellen	**Ereignisse**

4. Nachdem Sie die gewünschten Parameter der Richtlinie eingestellt haben, klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern.

19.4. Zeitgesteuerten Start für lokale Systemaufgaben deaktivieren/aktivieren

Mit Richtlinien können Sie auf allen Servern aus einer Administrationsgruppe das Gelten des Zeitplans für folgende lokale Systemaufgaben deaktivieren:

- **Echtzeitschutz für Dateien**
- **Skript-Untersuchung**
- Aufgaben zur Virensuche **Vollständige Untersuchung des Computers**, **Untersuchung von Quarantäne-Objekten, Integritätskontrolle für Anwendungen** und **Untersuchung bei Systemstart**
- Aufgaben zum Update **Update der Datenbanken**, **Update der Programm-Module** und **Update-Verteilung**.

Anmerkung

Wenn Sie einen geschützten Server aus der Administrationsgruppe ausschließen, wird der Zeitplan der Systemaufgaben automatisch aktiviert.

Um den zeitgesteuerten Start einer Systemaufgabe für Anti-Virus auf den Gruppenservern zu deaktivieren:

1. In der Administrationskonsole klappen Sie den Knoten **Gruppen** auf, dann die gewünschte Gruppe und dort gehen Sie auf den Knoten **Richtlinien**.

2. Öffnen Sie im Ergebnisfenster das Kontextmenü für die Richtlinie, mit deren Hilfe Sie den zeitgesteuerten Start von Systemaufgaben für Anti-Virus auf den Gruppenservern deaktivieren möchten, und wählen Sie den Befehl **Eigenschaften**.

3. Im Dialogfenster **Eigenschaften: <Richtlinie>** öffnen Sie die Registerkarte **Systemaufgaben** (s. Abbildung 101).

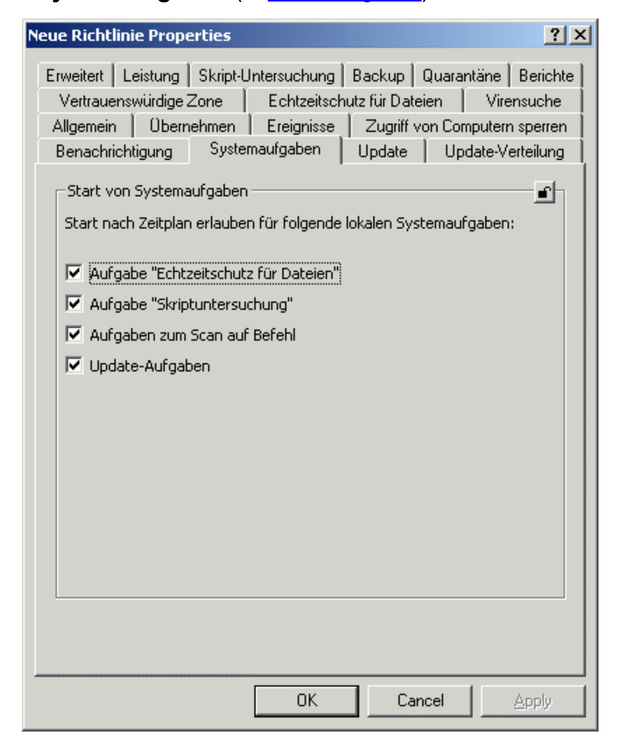


Abbildung 101. Dialogfenster **Eigenschaften: <Richtlinie>**, Registerkarte **Systemaufgaben**

4. Deaktivieren Sie das Kontrollkästchen neben dem Namen der Systemaufgabe, deren zeitgesteuerten Start Sie deaktivieren möchten.

Um den Zeitplan der Systemaufgabe erneut zu aktivieren, kreuzen Sie das Kontrollkästchen neben dem Namen der Aufgabe wieder an.

5. Klicken Sie auf die Schaltfläche **OK**.

Hinweis

Wenn der Start von zeitgesteuerten Systemaufgaben deaktiviert wurde, können die Aufgaben manuell aus der Anti-Virus-Konsole in der MMC sowie aus der Administrationskonsole von Kaspersky Administration Kit gestartet werden.

KAPITEL 20. ANTI-VIRUS IM DIALOGFENSTER EINSTELLUNGEN VON ANWENDUNG EINSTELLEN

In diesem Kapitel stehen die folgenden Informationen:

- Anti-Virus-Parameter einstellen (s. Pkt. 20.2 auf S. 302)
- Zugriff von Computern sperren (s. Pkt. 20.3 auf S. 306)
- Objekte in Quarantäne verwalten und Quarantäne-Parameter einstellen (s. Pkt. 20.4 auf S. 315)
- Dateien im Backup verwalten und Backup-Parameter einstellen (s. Pkt. 20.5 auf S. 318)
- Administrator- und Benutzerbenachrichtigungen über Anti-Virus-Ereignisse einstellen (s. Pkt. 20.6 auf S. 320)
- Vertrauenswürdige Prozesse verwalten (s. Pkt. 20.7 auf S. 323)

Wie das Dialogfensters **Einstellungen von Anwendung** geöffnet wird finden Sie in Pkt. 20.1 auf S. 300.

20.1. Dialogfenster *Einstellungen von Anwendung*

Im Dialogfenster **Einstellungen von Anwendung** können Sie Anti-Virus im Remote-Betrieb verwalten und Einstellungen auf dem geschützten Server vornehmen.

Um das Dialogfenster ***Einstellungen von Anwendung*** *zu öffnen, machen Sie Folgendes:*

1. In der Administrationskonsole klappen Sie den Knoten **Gruppen** auf und gehen auf die Gruppe, zu der der geschützte Server gehört.

2. In dem Ergebnisfenster öffnen Sie das Kontextmenü mit einem Rechtsklick auf die Zeile mit dem geschützten Server und gehen Sie auf **Eigenschaften**.

3. Im Dialogfenster **Eigenschaften: <Computer>** gehen Sie auf der Registerkarte **Anwendungen Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition** auf die Liste der installierten Anwendungen (s. Abbildung 102) und klicken Sie auf die Schaltfläche **Eigenschaften**.

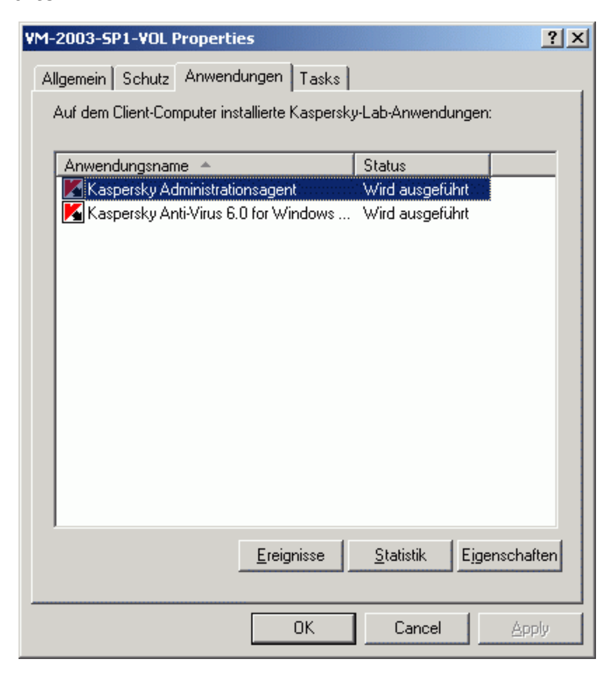


Abbildung 102. Liste mit Antiviren-Anwendungen im Dialogfenster **Eigenschaften: <Computer>**

Es öffnet sich das Dialogfenster **Einstellungen von Anwendung** (s. Abbildung 103).

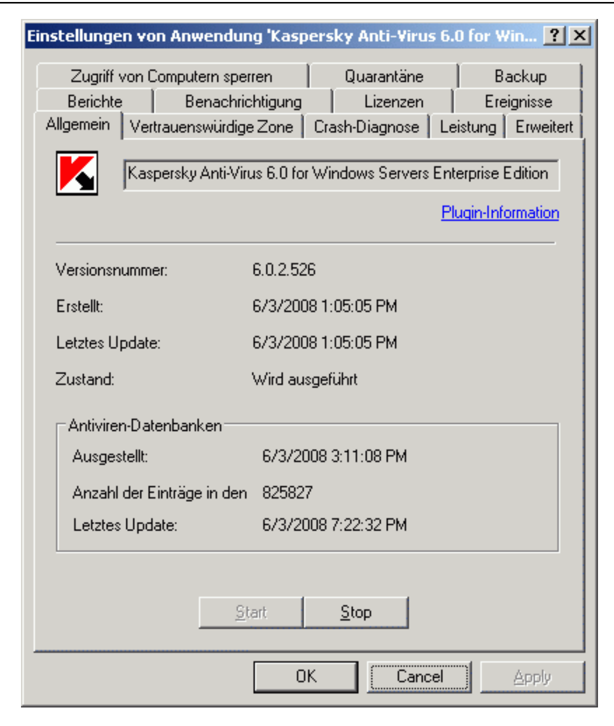


Abbildung 103. Dialogfenster **Einstellungen von Anwendung**, Registerkarte **Allgemein**

Anmerkung

Gilt eine Richtlinie von Kaspersky Administration Kit, lassen sich Parameterwerte, die in der Richtlinie mit dem Symbol 🔒 im Dialogfenster **Anwendungseigenschaften** der Administrationskonsole gekennzeichnet sind, sind ändern.

20.2. Einstellen der allgemeinen Anti-Virus-Parameter

Um die Anti-Virusparameter einzustellen, machen Sie Folgendes:

1. Öffnen Sie das Dialogfenster **Einstellungen von Anwendung** (s. Pkt. 20.1 auf S. 300).

   Auf den folgenden Registerkarten ändern Sie die Werte der allgemeinen Anti-Virus-Parameter je nach Ihren Wünschen.

- Auf der Registerkarte **Leistung** (s. Abbildung 104):
  - Tragen Sie die maximale Anzahl der Arbeitsprozesse ein, die vom Anti-Virus gestartet werden können (s. Pkt. B.1.1 auf S. 376).
  - Stellen Sie die fixe Anzahl der Prozesse für Aufgaben des Echtzeitschutzes ein (s. B.1.2 auf S. 377).
  - Stellen Sie die maximale Anzahl der Prozesse für Aufgaben zur Virensuche im Hintergrund ein (s. Pkt. B.1.3 auf S. 378).
  - Geben Sie die Anzahl der Versuche zur Wiederherstellung von Aufgaben nach einem Absturz von Aufgaben an (s. Pkt. B.1.4 auf S. 379).

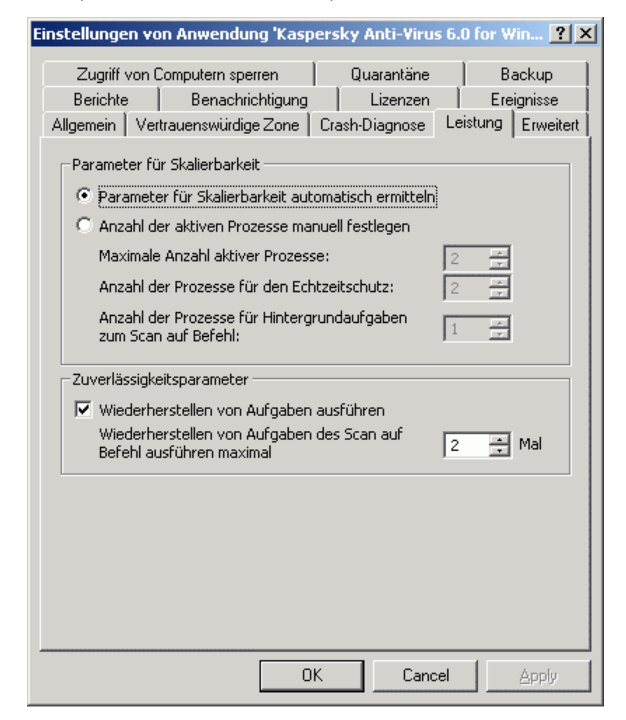


Abbildung 104. Dialogfenster **Einstellungen von Anwendung**, Registerkarte **Leistung**

- Auf der Registerkarte **Erweitert** (s. Abbildung 105):
  - Legen Sie fest, ob das Anti-Virus-Symbol im Infobereich der Taskleiste des Servers jedes Mal angezeigt werden soll, wenn Anti-Virus nach dem Neustart des Servers automatisch gestar-

tet wird (Details über das Anti-Virus-Symbol s. in Pkt. 2.4 auf S. 34).

- Geben Sie an, wie viele Tage Summen- und Detailberichte über die Aufgabenausführung gespeichert werden sollen, die im Knoten **Berichte** in der Anti-Virus-Konsole in der MMC dargestellt werden (s. Pkt. B.1.5 auf S. 380).
- Geben Sie an, wie lange Informationen gespeichert werden, die in der Anti-Virus-Konsole in der MMC im Knoten **Bericht zum System-Audit** dargestellt werden (s. Pkt. B.1.6 auf S. 380).
- Geben Sie die Aktionen des Anti-Virus beim Betrieb des Servers mit einer unterbrechungsfreien Stromversorgung an (s. Pkt. B.1.7 auf S. 381).
- Setzen Sie einen Grenzwert in Tagen, nach deren Ablauf die Ereignisse *Datenbanken sind veraltet*, *Datenbanken sind stark veraltet* und *Vollständige Untersuchung des Computers liegt lange zurück* eintreten (s. Pkt. B.1.8 auf S. 382).

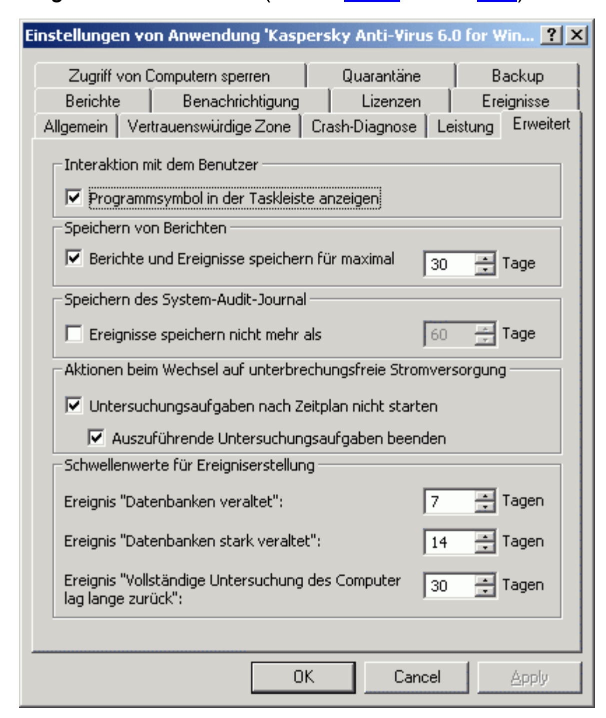


Abbildung 105. Dialogfenster **Einstellungen von Anwendung**, Registerkarte **Erweitert**

- Auf der Registerkarte **Crash-Diagnose** (s. Abbildung 106):
  - Aktivieren oder deaktivieren Sie das Protokoll der Ablaufverfolgung. Wenn das Erstellen eines Protokolls der Ablaufverfolgung aktiviert ist, stellen Sie die Parameter ein (s. Pkt. B.1.9 auf S. 382).
  - Aktivieren oder deaktivieren Sie die Dump-Dateien für Anti-Virus-Prozesse (s. Pkt. B.1.10 auf S. 388).

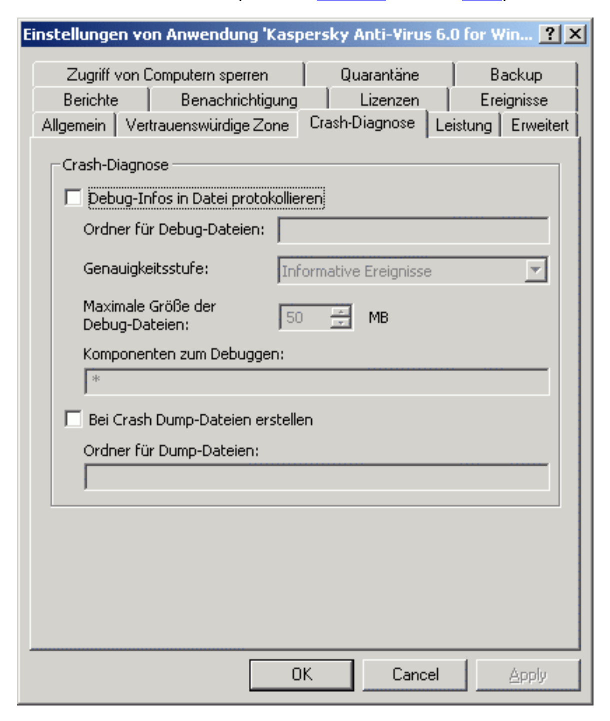


Abbildung 106. Dialogfenster **Einstellungen von Anwendung**, Registerkarte **Crash-Diagnose**

2. Nachdem Sie die Werte der gewünschten Anti-Virus-Parameter geändert haben, klicken Sie auf die Schaltfläche **OK**.

20.3. Zugriff von Computern sperren

Im Dialogfenster **Einstellungen von Anwendung** können Sie die Zugriffssperre für Computer und die Verhinderung von Virenepidemien verwalten (Details s. Pkt. 7.1 auf S. 96).

Sie können folgende Aktionen vornehmen:

- Parameter für automatische Zugriffssperre von Computern einstellen (s. Pkt. 20.3.1 auf S. 306)
- Computern in die Ausnahme-Liste für Sperrungen eintragen (s. Pkt. 20.3.3 auf S. 309)
- Aktivieren von Sicherheitsstufe automatisch erhöhen, wenn Anzahl der gesperrten Computer Grenzwert erreicht (Funktion *Virenepidemien verhindern*) (s. Pkt. 20.3.4 auf S. 310)
- Sperrliste anzeigen (s. Pkt. 20.3.5 auf S. 312)
- Zugriff von Computern per Hand sperren (s. Pkt. 20.3.6 auf S. 313)
- Zugriff von Computern freigeben (s. Pkt. 20.3.7 auf S. 314)

20.3.1. Automatische Zugriffssperre für Computer aktivieren/deaktivieren

Einzelheiten über die Funktion zur automatischen Zugriffssperre für Computer finden Sie unter B.4.1 auf S. 413.

> **Hinweis**
>
> Wenn Sie die Funktion zur automatischen Zugriffssperre von Computern aktivieren, wird sie nur dann ausgeführt, wenn die Aufgabe **Echtzeitschutz für Dateien** ausgeführt wird.

Um die Funktion zur automatischen Zugriffssperre für Computer zu aktivieren oder zu deaktivieren:

1. Öffnen Sie das Dialogfenster **Einstellungen von Anwendung** (s. Pkt. 20.1 auf S. 300).
2. Nehmen Sie auf der Registerkarte **Zugriff von Computern sperren** (s. Abbildung 107) eine der folgenden Aktionen vor:

- Um die Funktion zur automatischen Zugriffssperre von Computern einzuschalten, aktivieren Sie das Kontrollkästchen **Zugriffssperre für Computer auf den Server aktivieren**.
- Um die Funktion zur automatischen Zugriffssperre von Computern auszuschalten, deaktivieren Sie das Kontrollkästchen **Zugriffssperre für Computer auf den Server aktivieren**.

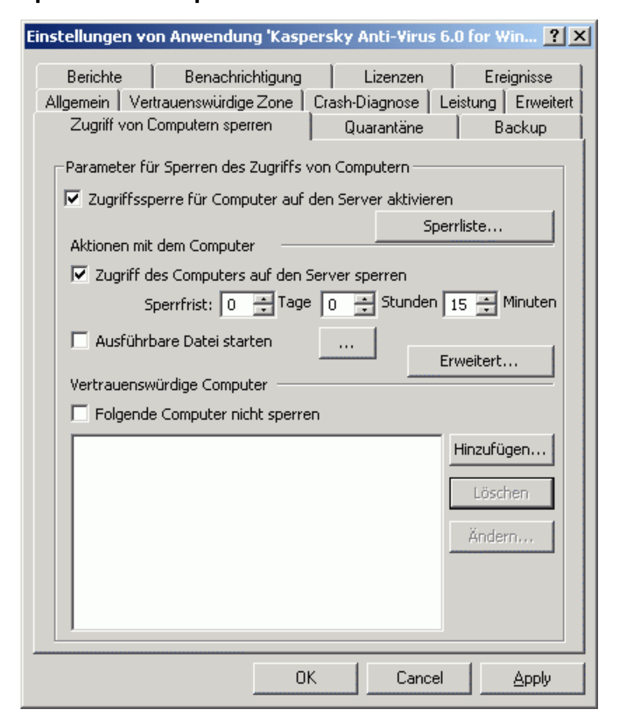


Abbildung 107. Dialogfenster **Einstellungen von Anwendung**, Registerkarte **Zugriff von Computern sperren**

20.3.2. Parameter für automatische Zugriffssperre von Computern einstellen

Um die Parameter für die automatische Zugriffssperre von Computern einzustellen, machen Sie Folgendes:

1. Öffnen Sie das Dialogfenster **Einstellungen von Anwendung** (s. Pkt. 20.1 auf S. 300).
2. Auf der Registerkarte **Zugriff von Computern sperren** (s. Pkt. B.4.1 auf S. 413) vergewissern Sie sich, dass das Häkchen in **Zugriffssperre für Computer auf den Server aktivieren** gesetzt ist (s. Pkt. B.4.2 auf S. 414).
3. In der Parametergruppe **Aktionen mit dem Computer** wählen Sie die Aktionen, die Anti-Virus ausführt, wenn von dem Computer aus ein infiziertes oder verdächtiges Objekt auf den Server geschrieben wird (s. Pkt. B.4.2 auf S. 414).
   - Wenn Sie **Zugriff des Computers auf den Server sperren** gewählt haben, dann geben Sie die Zeitspanne an, für die der Zugang auf den Server gesperrt wird, und zwar in Tagen, Stunden oder Minuten.
   - Wenn Sie **Ausführbare Datei starten** gewählt haben, dann klicken Sie auf die Schaltfläche ... und wählen Sie im Dialogfenster **Ausführbare Datei** (s. Abbildung 108) die ausführende Datei (Name und vollständiger Pfad zur Datei) sowie das Benutzerkonto, mit dessen Rechten die Datei ausgeführt werden soll.

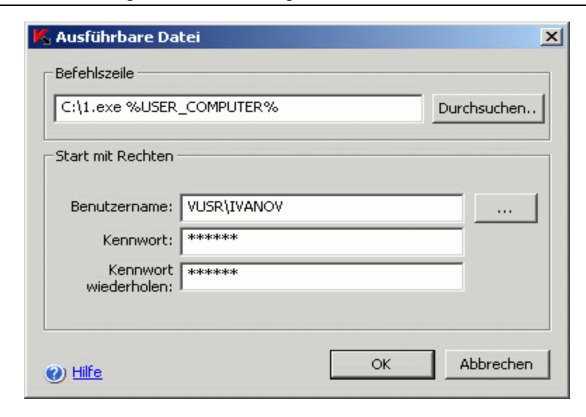


Abbildung 108. Dialogfenster **Ausführbare Datei**

4. Klicken Sie auf die Schaltfläche **OK** im Dialogfenster **Eigenschaften**.

20.3.3. Computer von Sperrung ausschließen (Vertrauenswürdige Computer)

Um einen Rechner zur Liste der vertrauenswürdigen Computer hinzuzufügen, machen Sie Folgendes (s. Pkt. B.4.3 auf S. 415):

1. Öffnen Sie das Dialogfenster **Einstellungen von Anwendung** (s. Pkt. 20.1 auf S. 300).
2. Auf der Registerkarte **Zugriff von Computern sperren** vergewissern Sie sich, dass das Häkchen in **Zugriffssperre für Computer auf den Server aktivieren** gesetzt ist (s. Pkt. B.4.1 auf S. 413).
3. In der Parametergruppe **Vertrauenswürdige Computer** setzen Sie das Häkchen in **Folgende Computern nicht sperren** und führen Sie folgende Aktionen durch:

   a) Klicken Sie auf die Schaltfläche **Hinzufügen** und geben Sie den Computer im Dialogfenster **Computer hinzufügen** an (s. Abbildung 109). Führen Sie eine der Aktionen durch:

      - Wählen Sie **Netzwerkname des Computers verwenden** und geben Sie den NetBIOS-Namen des Computers an.

- Geben Sie eine singuläre IP-Adresse ein: Wählen Sie **Netzwerk-IP-Adresse des Computers verwenden** und geben Sie die IP-Adresse des Computers ein.
- Ein IP-Adressbereich angeben: Wählen Sie **IP-Adressbereich verwenden**. Geben Sie die erste IP-Adresse des Bereichs in das Feld **Erste IP-Adresse**, und die letzte IP-Adresse in das Feld **Letzte IP-Adresse** ein. Alle Computer, deren IP-Adressen diesem Subnetz gehören, werden als Vertrauenswürdige Computer behandelt.

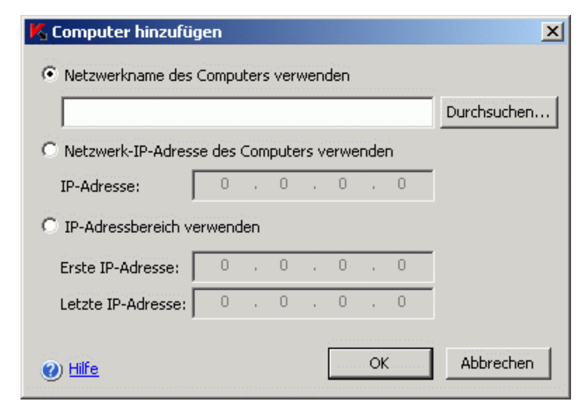


Abbildung 109. Dialogfenster **Computer hinzufügen**

b) Klicken Sie auf die Schaltfläche **OK**.

4. Klicken Sie auf die Schaltfläche **OK** im Dialogfenster **Eigenschaften**.

20.3.4. Virenepidemien verhindern

Sie können die Funktion *Virenepidemien verhindern* benutzen – wenn diese Funktion eingeschaltet ist, wird die Sicherheitsstufe automatisch erhöht, wenn die Anzahl der gesperrten Computer einen Grenzwert überschreitet (Funktion *Virenepidemien verhindern*).

Die Funktion *Virenepidemien verhindern* wird in Pkt. B.4.4 auf S. 416 näher beschrieben.

Um die Funktion Virenepidemien verhindern einzuschalten, machen Sie Folgendes:

1. Öffnen Sie das Dialogfenster **Einstellungen von Anwendung** (s. Pkt. 20.1 auf S. 300).

2. Auf der Registerkarte **Zugriff von Computern sperren** vergewissern Sie sich, dass das Häkchen in **Zugriffssperre für Computer auf den Server aktivieren** gesetzt ist.

3. Klicken Sie auf die Schaltfläche **Erweitert**.

4. Im Dialogfenster **Erweitert** (s. Abbildung 110) führen Sie eine der Aktionen durch:

   - Um die Funktion *Virenepidemien verhindern* zu aktivieren, machen Sie Folgendes:

     a) Setzen Sie das Häkchen in **Sicherheitsstufe erhöhen, wenn die Anzahl der Computer höher ist als**.

     b) Geben Sie die Anzahl der gesperrten Computer in der Liste der gesperrten Computer an, die erreicht werden muss, um die Sicherheitsstufe zu erhöhen.

     c) Schalten Sie die Wiederherstellung der Sicherheitsstufe ein oder aus, wenn die Anzahl der Computer, die gesperrt sind, bis zur vorgegebenen Anzahl sinkt. Geben Sie die Anzahl in dem Feld **Sicherheitsstufe wiederherstellen, wenn die Anzahl der Computer geringer ist als** an.

   - Um die Funktion *Virenepidemien verhindern* abzuschalten, entfernen Sie das Häkchen in **Sicherheitsstufe erhöhen, wenn die Anzahl der Computer höher ist als**.

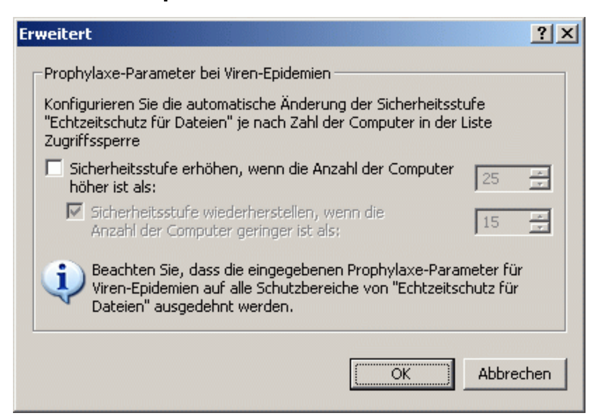


Abbildung 110. Dialogfenster **Erweitert**

5. Klicken Sie auf die Schaltfläche **OK**.

6. Klicken Sie auf die Schaltfläche **OK** im Dialogfenster **Eigenschaften**.

20.3.5. Sperrliste anzeigen

Achtung!

Computern in der Sperrliste wird der Zugang zum geschützten Server erst gesperrt, wenn die Aufgabe **Echtzeitschutz für Dateien** läuft und die Funktion automatische Zugriffssperre von Computern aktiviert ist.

Um die Computerliste anzuzeigen, für die der Zugang zum geschützten Server momentan gesperrt ist, machen Sie Folgendes:

1. Öffnen Sie das Dialogfenster **Einstellungen von Anwendung** (s. Pkt. 20.1 auf S. 300).
2. Auf der Registerkarte **Zugriff von Computern sperren** klicken Sie auf die Schaltfläche **Sperrliste** (s. Abbildung 111).

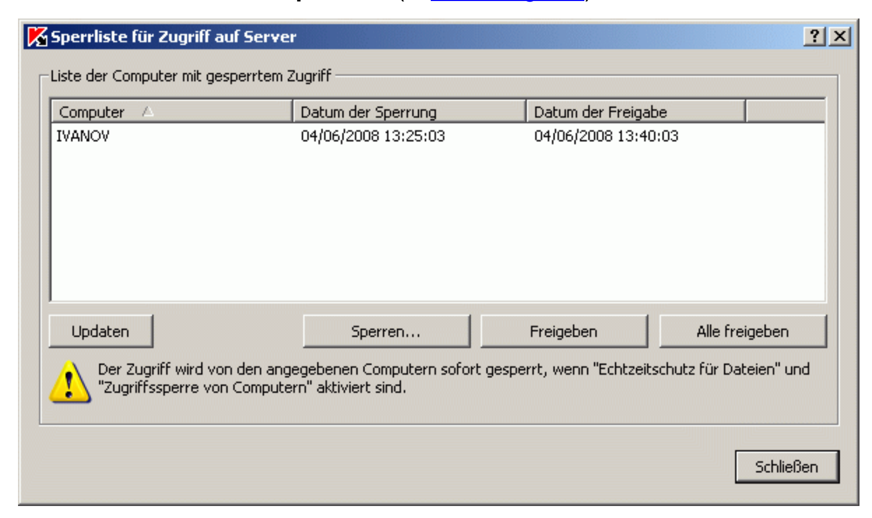


Abbildung 111. Dialogfenster **Sperrliste für Zugriff auf Server**

Im Dialogfenster **Sperrliste** werden die folgenden Informationen über Computer angezeigt, für die zurzeit der Zugang zum geschützten Server gesperrt ist:

Feld	Beschreibung
Computer	Informationen über den Computer in der Sperrliste. Diese Informationen wurden von Anti-Virus bei der Identifikation des Computers ermittelt (Netzwerkname, IP-Adresse des Computers)

Feld	Beschreibung
Datum der Sperrung	Datum und Uhrzeit, wann der Zugang für den Computer gesperrt wurde; wird entsprechend dem Format in den Regionsoptionen von Microsoft Windows angezeigt, die auf dem Computer mit der Administrationskonsole benutzt werden.
Datum der Freigabe	Datum und Uhrzeit, wann der Zugang zum Server für dem Computer freigegeben wird; wird entsprechend dem Format in den Regionsoptionen von Microsoft Windows angezeigt, die auf dem Computer mit der Administrationskonsole benutzt werden.

20.3.6. Zugriff von Computern von Hand sperren

Wenn Sie Informationen darüber haben, dass ein Computer im lokalen Netzwerk infiziert ist, dann können Sie für diesen Computer den Zugang zum geschützten Server per Hand sperren.

Achtung!

Computern in der Sperrliste wird der Zugang zum geschützten Server erst gesperrt, wenn die Aufgabe **Echtzeitschutz für Dateien** läuft und die Funktion automatische Zugriffssperre von Computern aktiviert ist.

Um den Zugriff auf den Server von einem Computer zu sperren:

1. Öffnen Sie das Dialogfenster **Einstellungen von Anwendung** (s. Pkt. 20.1 auf S. 300).
2. Auf der Registerkarte **Zugriff von Computern sperren** klicken Sie auf die Schaltfläche **Sperrliste**.
3. Im Dialogfenster **Sperrliste** klicken Sie auf **Sperren**.
4. Im Dialogfenster **Zugang eines Computers sperren** (s. Abbildung 112) geben Sie den Netzwerknamen des Computers an, für den der Zugang gesperrt werden soll.

Hinweis

Geben Sie im Feld **Name des Computers** nur die Netzwerk-NetBIOS-Namen der Computer an, nicht die DNS-Adressen.



Abbildung 112. Dialogfenster **Zugang eines Computers sperren**

5. Führen Sie danach eine der folgenden Aktionen durch:

   - Wählen Sie **Zugriff des Computers auf den Server sperren für** und geben Sie die Zeitperiode an, für die der Zugang des Computers zum Server gesperrt werden soll.
   - Wählen Sie **Zugriff des Computers auf den Server sperren bis zum folgenden Datum** und geben Sie Datum und Uhrzeit an, wann der Computer freigegeben werden soll.

   Anmerkung

   Geben Sie Datum und Uhrzeit bezüglich aktuellen Datum und Uhrzeit des geschützten Servers an.

6. Klicken Sie auf **OK**.
7. Klicken Sie auf die Schaltfläche **OK** im Dialogfenster **Eigenschaften**.

20.3.7. Freigabe des Zugriffs von Computern

Um den Zugriff von einem Computer freizugeben:

1. Öffnen Sie das Dialogfenster **Einstellungen von Anwendung** (s. Pkt. 20.1 auf S. 300).
2. Auf der Registerkarte **Zugriff von Computern sperren** klicken Sie auf die Schaltfläche **Sperrliste**.

3. Im Dialogfenster **Sperrliste** markieren Sie den Computer, der Sie freigeben möchten, und klicken Sie auf die Schaltfläche **Computer entsperren**.

   Um alle gesperrten Computer freizugeben, klicken Sie auf die Schaltfläche **Alle freigeben**.

4. Klicken Sie auf **OK**.
5. Klicken Sie auf die Schaltfläche **OK** im Dialogfenster **Eigenschaften**.

20.4. Objekte in der Quarantäne verwalten und Quarantäne-Parameter einstellen

20.4.1. Quarantänefunktionen und Einstellungswerkzeuge

In folgender Tabelle sind Funktionen der Quarantäne und Administrationswerkzeuge aufgeführt. Mit den Werkzeugen können Sie die Funktionen verwalten.

Tabelle 27. Quarantänefunktionen und Einstellungswerkzeuge

Quarantänefunktion	**Administrationskonsole von Kaspersky Administration Kit**	**Anti-Virus-Konsole in der MMC**
Ansicht, Sortierung und Objektentfernung	Ja (s. *Kaspersky Administration Kit. Administratorhandbuch*)	Ja
Objektfilterung	Nein	Ja
Verdächtige Objekte aus Quarantäne zur Analyse in Virenlabor einschicken	Nein	Ja

Quarantänefunktion	Administrationskonsole von Kaspersky Administration Kit	Anti-Virus-Konsole in der MMC
Objekte per Hand in Quarantäne verschieben	Nein	Ja
Objekte aus der Quarantäne wiederherstellen	Ja (nur in den ursprünglichen Pfad)	Ja
Objekte in der Quarantäne untersuchen	Ja Aufgabe **Untersuchung von Quarantäne-Objekten** starten	Ja
Einstellung der Quarantäne-Parameter	Ja s. Pkt. 20.4.2 auf S. 316	Ja
Statistik für Quarantäne anzeigen	Ja s. Anti-Virus-Statistik anzeigen, Pkt. 18.3 auf S. 280.	Ja

20.4.2. Quarantäne-Parameter einstellen

Im Dialogfenster **Einstellungen von Anwendung** des ausgewählten geschützten Servers können Sie die Quarantäne-Parameter einstellen.

Informationen über die Isolation von verdächtigen Objekten finden Sie in Pkt. 11.1 auf S. 170.

Um die Quarantäne-Parameter einzustellen, machen Sie Folgendes:

1. Öffnen Sie das Dialogfenster **Einstellungen von Anwendung** (s. Pkt. 20.1 auf S. 300).
2. Auf der Registerkarte **Quarantäne** (s. Abbildung 113) ändern Sie bei Bedarf die Quarantäne-Parameter:
   - Um einen anderen Ordner für die Quarantäne auszuwählen, wählen Sie im Feld **Quarantäne-Ordner** einen gewünschten Ordner

auf dem Datenträger aus oder geben Sie den vollständigen Pfad per Hand ein (s. Pkt. B.6.1 auf S. 430).

- Um die maximale Größe der Quarantäne zu begrenzen, setzen Sie das Häkchen in **Maximale Größe der Quarantäne** und tragen Sie im Eingabefeld den gewünschten Parameterwert in Megabyte ein (s. Pkt. B.6.2 auf S. 431).
- Um die minimale Größe des freien Speicherplatzes in der Quarantäne anzugeben, setzen Sie das Häkchen in **Maximale Größe der Quarantäne**, setzen Sie das Häkchen in **Grenzwert für freien Speicherplatz** und tragen Sie den gewünschten Parameterwert in Megabyte ein (s. Pkt. B.6.3 auf S. 432).
- Um einen anderen Ordner für wiederhergestellte Objekte auszuwählen, wählen Sie in der Parametergruppe **Parameter für die Wiederherstellung von Objekten** den gewünschten Ordner auf dem Datenträger aus oder geben sie den vollständigen Pfad per Hand ein. (s. Pkt. B.6.4 auf S. 432).

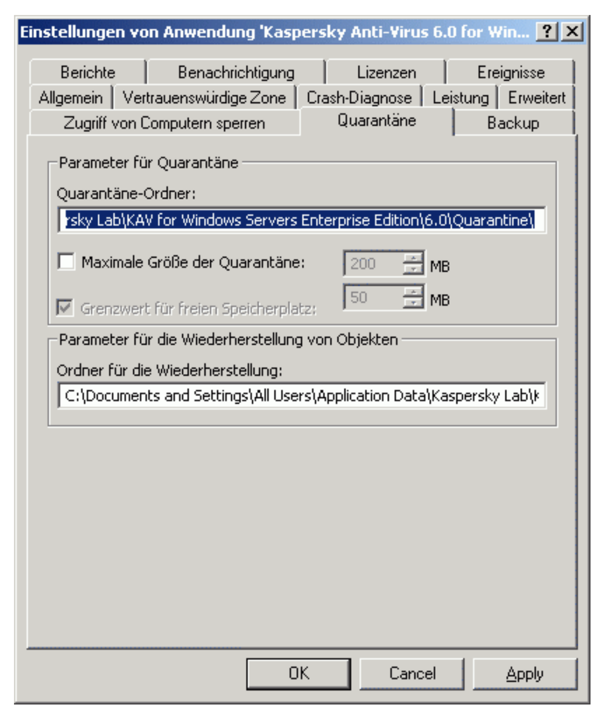


Abbildung 113. Dialogfenster **Einstellungen von Anwendung**, Registerkarte **Quarantäne**

3. Klicken Sie auf die Schaltfläche **OK**.

20.5. Dateien im Backup verwalten und Backup-Parameter einstellen

20.5.1. Backup-Funktionen und -Einstellung

In folgender Tabelle sind die Backup-Funktionen aufgezählt und die Administrationswerkzeuge angegeben, mit denen dessen Funktionen verwalten werden können.

Tabelle 28. Backup-Funktionen

Backup-Funktion	Administrationskonsole von Kaspersky Administration Kit	Anti-Virus-Konsole in der MMC
Anzeigen, Sortieren und Löschen von Dateien	Ja	Ja
Dateien filtern	Nein	Ja
Dateien aus dem Backup wiederherstellen	Ja (Nur im ursprünglichen Pfad)	Ja
Backup-Parameter einstellen	Ja s. Pkt. 20.5.2 auf S. 319	Ja
Statistik für Backup ansehen	Ja s. Anti-Virus-Statistik anzeigen, Pkt. 18.3 auf S. 280 .	Ja

20.5.2. Backup-Parameter einstellen

Im Dialogfenster **Einstellungen von Anwendung** des ausgewählten geschützten Servers können Sie die Backup-Parameter einstellen.

Über Sicherungskopien von Objekten vor dem Desinfizieren oder Löschen finden Sie mehr in Pkt. 12.1 auf S. 189.

Um die Backup-Parameter einzustellen, machen Sie Folgendes:

1. Öffnen Sie das Dialogfenster **Einstellungen von Anwendung** (s. Pkt. 20.1 auf S. 300), öffnen Sie die Registerkarte **Backup**.
2. Auf der Registerkarte **Backup** stellen Sie die gewünschten Backup-Parameter ein (s. Abbildung 114):
   - Um einen anderen Backup-Ordner anzugeben, wählen Sie im Feld **Maximale Größe des Backups** einen gewünschten Ordner auf dem Datenträger aus oder geben Sie den vollständigen Pfad per Hand ein (s. Pkt. B.7.1 auf S. 434).
   - Um die maximale Größe des Backups zu ändern, setzen Sie das Häkchen in **Maximale Größe des Backups** und geben Sie den Wert in Megabyte an (s. Pkt. B.7.2 auf S. 435).
   - Um die minimale Größe des freien Speicherplatzes im Backup anzugeben, setzen Sie das Häkchen in **Maximale Größe des Backups**, setzen Sie das Häkchen in **Grenzwert für freien Speicherplatz** und tragen Sie den gewünschten Parameterwert in Megabyte ein (s. Pkt. B.7.3 auf S. 435).
   - Um einen anderen Ordner für wiederhergestellte Objekte auszuwählen, wählen Sie in der Parametergruppe **Parameter für die Wiederherstellung von Objekten** den gewünschten Ordner auf dem Datenträger aus oder geben sie den vollständigen Pfad per Hand ein (s. Pkt. B.7.4 auf S. 436).

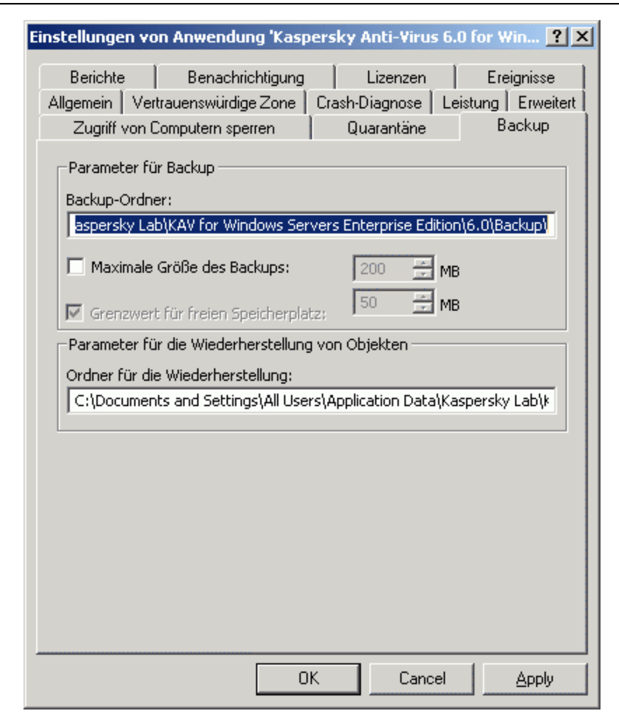


Abbildung 114. Dialogfenster **Einstellungen von Anwendung**, Registerkarte **Backup**

3. Klicken Sie auf die Schaltfläche **OK**.

20.6. Benachrichtigungen einstellen

In diesem Abschnitt stehen die folgenden Informationen:

- allgemeine Informationen über die Einstellung von Benachrichtigungen über die Administrationskonsole (s. Pkt. 20.6.1 auf S. 321)
- Administrator- und Benutzerbenachrichtigungen auf der Registerkarte *Benachrichtigung* einstellen (s. Pkt. 20.6.2 auf S. 322)

20.6.1. Allgemeines

In der Administrationskonsole von Kaspersky Administration Kit können Benachrichtigungen für Administratoren und Benutzer eingestellt werden, die über die Arbeit des Anti-Virus und Schutzzustand des geschützten Servers informieren:

- Der Administrator kann Informationen über Ereignisse bestimmter Typen erhalten.
- Die Netzwerkbenutzer, welche den geschützten Server ansprechen, können Informationen über Ereignisse *Bedrohung gefunden* und *Computer wurde in Sperrliste eingefügt* erhalten; Terminal-Benutzer können Information über Ereignis *Bedrohung gefunden* erhalten.

Die Benachrichtigungen über Anti-Virus-Ereignisse können sowohl für einen Server im Fenster **Einstellungen von Anwendung** des ausgewählten Servers eingestellt werden, wie auch für eine Servergruppe im Fenster **Eigenschaften: <Richtlinie>** der gewählten Gruppe.

In den Dialogfenstern können Sie die Benachrichtigungen auf der Registerkarte **Ereignisse** oder auf der Registerkarte **Benachrichtigung** einstellen.

- Auf der Registerkarte **Ereignisse** (standardmäßige Registerkarte von Kaspersky Administration Kit) können Sie die Benachrichtigungen für den Administrator über ausgewählte Ereignistypen einstellen. Welche Benachrichtigungsmöglichkeiten Sie haben und wie diese eingestellt werden, erfahren Sie im Dokument *Kaspersky Administration Kit. Administratorhandbuch*.
- Auf der Registerkarte **Benachrichtigung** können Sie Benachrichtigungen für den Administrator und für Benutzer einstellen. Details darüber, welche Benachrichtigungsmöglichkeiten Sie auf der Registerkarte **Benachrichtigung** einstellen können, finden Sie in Pkt. 15.1 auf S. 235. Wie Benachrichtigungen auf der Registerkarte **Benachrichtigung** eingestellt werden, finden Sie in Pkt. 20.6.2 auf S. 322.

Die Benachrichtigungen über Ereignisse einiger Typen können nur auf einer der Registerkarten eingestellt werden. Ereignisse anderer Typen lassen sich auf beiden Registerkarten einstellen.

Anmerkung

Wenn Sie Ereignis-Benachrichtigungen gleichen Typs auf eine Weise gleichzeitig auf zwei Registerkarten einstellen, das heißt auf der Registerkarte **Ereignisse** und auf der Registerkarte **Benachrichtigung**, dann bekommt Administrator diese Benachrichtigung zwei Mal.

20.6.2. Benachrichtigungen für Administrator und Benutzer auf Registerkarte *Benachrichtigung*

Um Benachrichtigungen einzustellen, machen Sie Folgendes:

1. Öffnen Sie das Dialogfenster **Einstellungen von Anwendung** (s. Pkt. 20.1 auf S. 300), öffnen Sie die Registerkarte **Benachrichtigung**.
2. Auf der Registerkarte **Benachrichtigung** (s. Abbildung 115) stellen Sie die Ereignis-Benachrichtigungen der gewünschten Typen ein und klicken Sie auf die Schaltfläche **OK**.

Das Einstellen von Benachrichtigungen auf der Registerkarte **Benachrichtigung** gleicht dem Einstellen von Benachrichtigungen im Dialogfenster **Benachrichtigungen** der Anti-Virus-Konsole in der MMC. Details dazu finden Sie in Pkt. 15.2 auf S. 237.

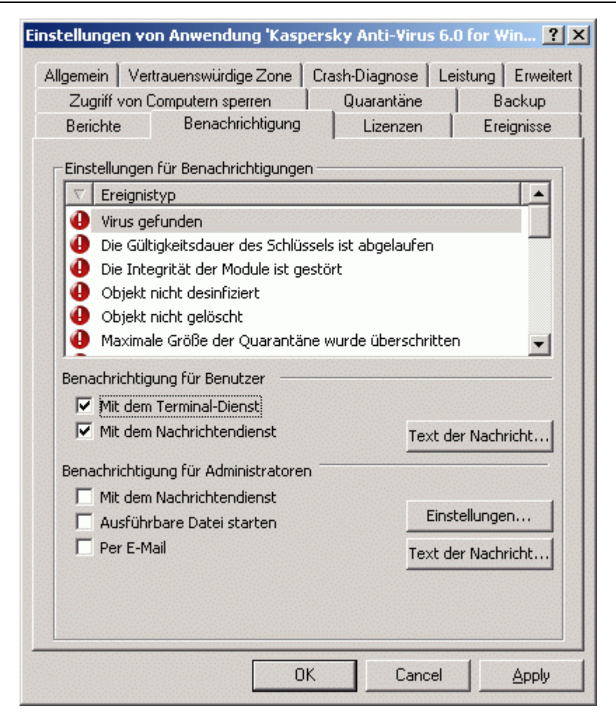


Abbildung 115. Dialogfenster **Einstellungen von Anwendung**, Registerkarte **Benachrichtigung**

20.7. Vertrauenswürdige Prozesse verwalten

Dieser Abschnitt enthält folgende Informationen:

- Hinzufügen von Prozessen zur Liste der vertrauenswürdigen Prozesse (s. Pkt. 20.7.1 auf S. 324);
- Abschalten des Echtzeitschutzes für Dateien während dem Anlegen von Sicherungskopien (s. Pkt. 20.7.2 auf S. 326);
- Hinzufügen von Ausnahmen (s. Pkt. 20.7.3 auf S. 327);
- Übernehmen der vertrauenswürdigen Zone (s. Pkt. 20.7.4 auf S. 331).

Details zur vertrauenswürdigen Zone von Anti-Virus finden Sie in Pkt. 8.1 auf S. 109.

20.7.1. Prozesse zur vertrauenswürdigen Liste hinzufügen

In der Administrationskonsole von Kaspersky Administration Kit können Sie ausführbare Dateien von Prozessen, die sich auf dem Laufwerk eines geschützten Servers befinden, zur vertrauenswürdigen Zone hinzufügen. Sie können keine Prozesse aus der Liste der auf dem Server aktiven Prozesse hinzufügen.

Details zur vertrauenswürdigen Zone finden Sie Pkt. 8.1 auf S. 109.

Um einen Prozess zur Liste der Vertrauenswürdigen Prozesse hinzuzufügen, machen Sie Folgendes:

1. Öffnen Sie das Dialogfenster **Einstellungen von Anwendung** (s. Pkt. 20.1 auf S. 300), Registerkarte **Vertrauenswürdige Zone** (s. Abbildung 116).

2. Schalten Sie die Funktion **Vertrauenswürdige Prozesse** ein: Setzen Sie Häkchen in **Datei-Aktivität der angegebenen Prozesse nicht untersuchen**.

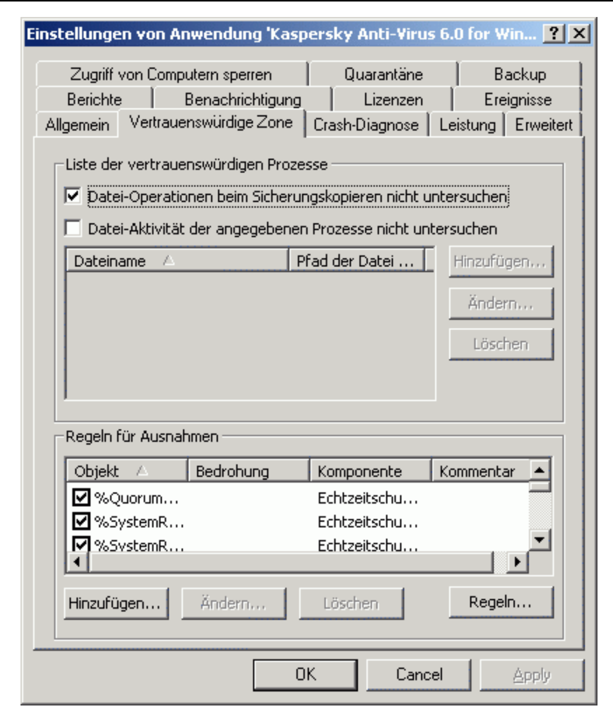


Abbildung 116. Dialogfenster **Einstellungen von Anwendung**, Registerkarte **Vertrauenswürdige Zone**

3. Um eine ausführende Datei auf einem der Datenträger des geschützten Servers auszuwählen, machen Sie Folgendes:

    a) Auf der Registerkarte **Vertrauenswürdige Zone** klicken Sie auf die Schaltfläche **Hinzufügen**.

    b) Im Dialogfenster **Vertrauenswürdigen Prozess hinzufügen** klicken Sie auf **Durchsuchen** und wählen Sie die ausführende Prozessdatei auf dem lokalen Datenträger des geschützten Servers. Im Dialogfenster **Vertrauenswürdigen Prozess hinzufügen** werden der Dateiname und der Pfad angezeigt.

    c) Klicken Sie auf die Schaltfläche **OK**.

    Der Name der ausgewählten ausführenden Datei wird in die Liste auf der Registerkarte **Vertrauenswürdige Zone** angezeigt.

4. Klicken Sie auf **OK**, um die Änderungen zu übernehmen.

20.7.2. Echtzeitschutz für Dateien während dem Anlegen von Sicherungskopien ausschalten

Sie können den Echtzeitschutz für Dateien, auf die bei Operationen zum Sicherungskopieren zugegriffen wird, während dem Anlegen von Sicherungskopien ausschalten. Anti-Virus untersucht Dateien nicht, die von einem Backup-Programm mit dem Attribut FILE_FLAG_BACKUP_SEMANTICS zum Lesen geöffnet werden.

Um den Echtzeitschutz für Dateien während des Anlegens von Sicherungskopien zu deaktivieren:

1. Öffnen Sie das Dialogfenster **Einstellungen von Anwendung** (s. Pkt. 20.1 auf S. 300) auf der Registerkarte **Vertrauenswürdige Zone** (s. Abbildung 117).

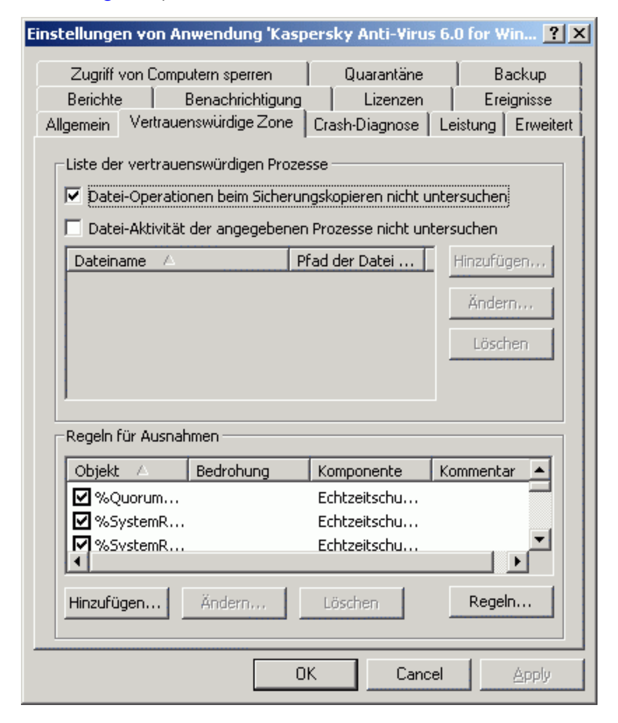


Abbildung 117. Dialogfenster **Einstellungen von Anwendung**, Registerkarte **Vertrauenswürdige Zone**

2. Um Echtzeitschutz für Dateien abzuschalten, welche vom Backup kopiert werden, setzen Sie Häkchen **Datei-Operationen beim Sicherungskopien nicht untersuchen**.
3. Klicken Sie auf **OK**, um Änderungen zu speichern.
4. Übernehmen Sie die Ausnahmen der vertrauenswürdigen Zone in den ausgewählten Aufgaben und Richtlinien (s. Pkt. 20.7.4 auf S. 331).

20.7.3. Ausnahmen zur vertrauenswürdigen Zone hinzufügen

Sie können der vertrauenswürdigen Zone Objekte hinzufügen, die von der Untersuchung ausgeschlossen werden sollen. Details zur vertrauenswürdigen Zone finden Sie in Pkt. 8.1 auf S. 109.

Um eine Ausnahme hinzuzufügen:

1. Öffnen Sie das Dialogfenster **Einstellungen von Anwendung** (s. Pkt. 20.1 auf S. 300) auf der Registerkarte **Vertrauenswürdige Zone** (s. Abbildung 116).
2. Klicken Sie im Abschnitt **Ausnahmen** auf die Schaltfläche **Hinzufügen**.

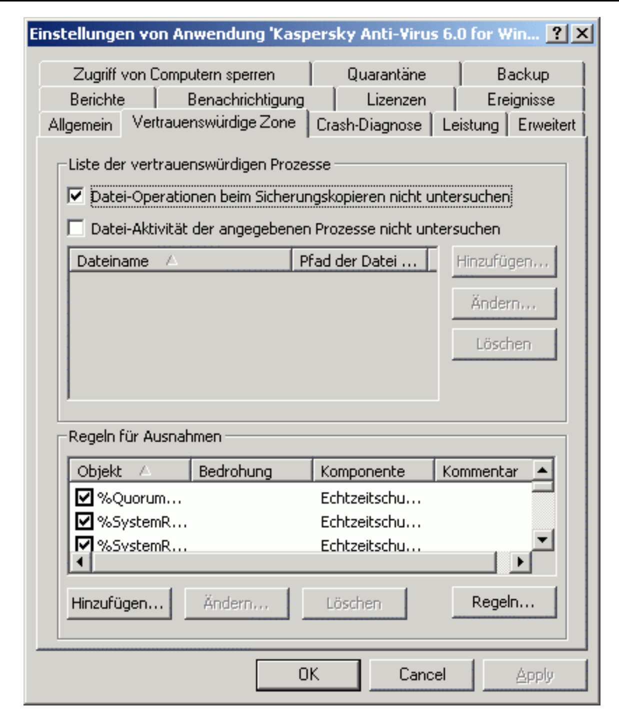


Abbildung 118. Dialogfenster **Einstellungen von Anwendung**, Registerkarte **Vertrauenswürdige Zone**

Das Dialogfenster **Ausnahmeregel** wird geöffnet.

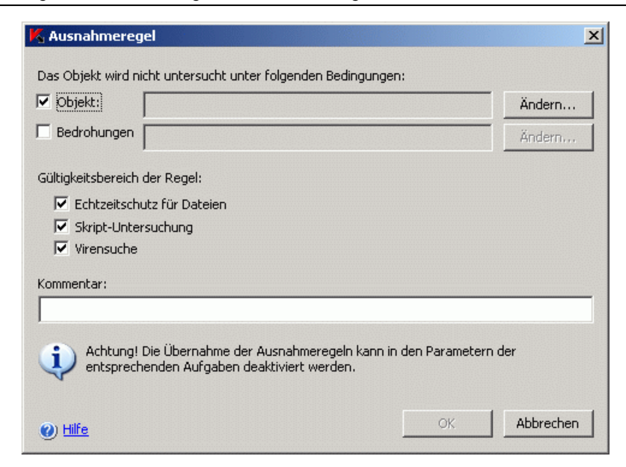


Abbildung 119. Dialogfenster **Ausnahmeregel**

3. Geben Sie die Regel an, nach der Anti-Virus das Objekt ausschließen soll.

> **Hinweis**
>
> Um *festgelegte Bedrohungen in bestimmten Ordnern oder Dateien* auszuschließen, aktivieren Sie die Kontrollkästchen **Objekt** und **Bedrohungen**.
>
> Um *alle Bedrohungen in bestimmten Ordnern oder Dateien* auszuschließen, aktivieren Sie das Kontrollkästchen **Objekt** und deaktivieren Sie das Kontrollkästchen **Bedrohungen**.
>
> Um festgelegte *Bedrohungen im gesamten Untersuchungsbereich* auszuschließen, deaktivieren Sie das Kontrollkästchen **Objekt** und aktivieren Sie das Kontrollkästchen.

- Wenn Sie *den Pfad des Objekts festlegen möchten,* aktivieren Sie das Kontrollkästchen **Objekt**, klicken Sie auf **Ändern**, geben Sie im Dialogfenster **Objekt wählen** (s. Abbildung 39) das Objekt an, das von der Untersuchung ausgeschlossen werden soll, und klicken Sie anschließend auf **OK**:
  - **Vordefinierter Untersuchungsbereich**. Wählen Sie einen vordefinierten Untersuchungsbereich aus der Liste aus.
  - **Laufwerk oder Ordner**. Geben Sie ein Serverlaufwerk oder einen Ordner auf dem Server oder im lokalen Netzwerk an.
  - **Datei**. Geben Sie eine Datei auf dem Server oder im lokalen Netzwerk an.

- **Datei oder URL-Adresse eines Skripts**. Geben Sie ein Skript auf dem geschützten Server, im lokalen Netzwerk oder im Internet an.

Hinweis

Bei der Angabe von Masken für Ordner- und Dateinamen können die Zeichen ? und * verwendet werden.

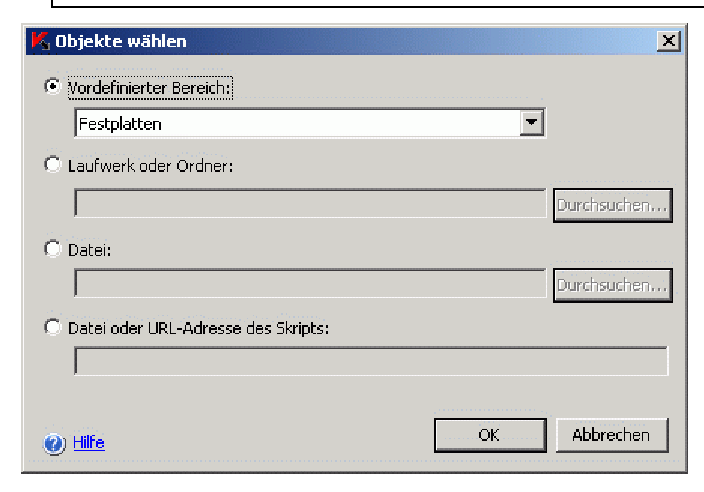


Abbildung 120. Dialogfenster **Objekt wählen**

- *Wenn Sie den Namen einer Bedrohung festlegen möchten*, aktivieren Sie die Kontrollkästchen **Bedrohungen**, klicken Sie auf **Ändern** und fügen Sie im Dialogfenster **Liste der Ausnahmen** den Namen der Bedrohung hinzu (Details zu diesem Parameter finden Sie in Pkt. B.3.9 auf S. 408).

4. Aktivieren Sie die Kontrollkästchen neben den Namen der funktionalen Komponenten, in deren Aufgaben die Ausnahmeregel übernommen werden soll.

5. Klicken Sie auf **OK**.

- Um eine Regel anzupassen, wählen Sie die betreffende Regel auf der Registerkarte **Vertrauenswürdige Zone** aus, klicken Sie auf **Ändern** und *nehmen* Sie im Dialogfenster **Ausnahmeregel** die entsprechenden Änderungen vor.

- Um eine Regel zu löschen, wählen Sie die betreffende Regel auf der *Registerkarte* **Vertrauenswürdige Zone** aus, klicken Sie auf **Löschen** und bestätigen Sie die Operation.

6. Klicken Sie im Dialogfenster **Einstellungen von Anwendung** auf **OK**.
7. Falls erforderlich, übernehmen Sie die Ausnahmen der vertrauenswürdigen Zone in den ausgewählten Aufgaben und Richtlinien (s. Pkt. 20.7.4 auf S. 331).

20.7.4. Vertrauenswürdige Zone übernehmen

Sie können das Übernehmen der vertrauenswürdigen Zone in den vorhandenen Richtlinien sowie in den Aufgaben aktivieren oder deaktivieren (beim Erstellen einer Aufgabe oder im Dialogfenster **Eigenschaften: Aufgabe**).

Die vertrauenswürdige Zone wird standardmäßig in neu erstellten Richtlinien und Aufgaben übernommen.

Um die vertrauenswürdige Zone in einer Richtlinie zu übernehmen:

1. Öffnen Sie in der Struktur der Administrationskonsole den Knoten **Gruppen**. Öffnen Sie dann in der Administrationsgruppe die Eigenschaften der betreffenden Richtlinie. Öffnen Sie anschließend den untergeordneten Knoten **Richtlinien**.
2. Öffnen Sie im Detailfenster das Kontextmenü für die Richtlinie, deren Parameter Sie anpassen möchten, und wählen Sie den Befehl **Eigenschaften**.
3. Führen Sie im Dialogfenster **Eigenschaften: <Richtlinie>** folgende Aktionen aus:
   - Zum Übernehmen einer Ausnahme: *Vertrauenswürdige Prozesse*, vergewissern Sie sich, dass das Kontrollkästchen **Datei-Aktivität der angegebenen Prozesse nicht untersuchen** aktiviert ist und aktivieren Sie das Schloss in der Parametergruppe **Liste der vertrauenswürdigen Prozesse**.
   - Zum Übernehmen einer Ausnahme: *Vorgänge des Sicherungskopierens*, vergewissern Sie sich, dass das Kontrollkästchen **Datei-Operationen beim Sicherungskopieren nicht untersuchen** aktiviert ist und aktivieren Sie das Schloss in der Parametergruppe **Liste der vertrauenswürdigen Prozesse**.
   - Um *Ausnahmen, die der Benutzer angegeben hat* zu übernehmen, aktivieren Sie das Schloss in der Parametergruppe **Ausnahmen**..
4. Klicken Sie auf **OK**.

Um die vertrauenswürdige Zone in einer vorhandenen Aufgabe zu übernehmen:

1. Öffnen Sie in der Struktur der Administrationskonsole den Knoten **Gruppen** und wählen Sie die Gruppe aus, die zu dem geschützten Server gehört.

2. Öffnen Sie im Detailfenster das Kontextmenü für die Zeile mit Informationen über den geschützten Server und wählen Sie den Befehl **Eigenschaften**.

3. Öffnen Sie im Dialogfenster **Eigenschaften: <Computer>** auf der Registerkarte **Aufgaben** das Kontextmenü für die Aufgabe, die Sie anpassen möchten, und wählen Sie den Befehl **Eigenschaften**.

4. Klicken Sie im Dialogfenster **Eigenschaften: <Aufgabe>** auf der Registerkarte **Einstellungen** auf die Schaltfläche **Erweitert** und aktivieren Sie im Dialogfenster **Erweitert** das Kontrollkästchen **Vertrauenswürdigen Zone anwenden.**

   Die vertrauenswürdige Zone kann auch beim Erstellen einer Aufgabe übernommen werden.

KAPITEL 21. AUFGABEN ERSTELLEN UND EINSTELLEN

In diesem Kapitel stehen die folgenden Informationen:

- Aufgabentypen, die in der Administrationskonsole erstellt werden können (s. Pkt. 21.1 auf S. 333)
- Aufgaben erstellen (s. Pkt. 21.2 auf S. 334)
- Aufgabe einstellen (s. Pkt. 21.3 auf S. 344)

21.1. Aufgaben erstellen

Sie können lokale benutzerdefinierte Aufgaben, Gruppenaufgaben und globale Aufgaben folgenden Typs erstellen:

- Virensuche
- Aufgaben zum Update
- Rollback des Updates der Datenbanken
- Schlüssel installieren

Sie stellen lokale Aufgaben für den ausgewählten geschützten Server im Dialogfenster **Einstellungen von Anwendung** auf der Registerkarte **Aufgaben**, Gruppenaufgaben im Knoten **Gruppenaufgabe** der ausgewählten Gruppe, globale Aufgaben im Knoten **Globale Aufgaben**.

> **Anmerkung**
>
> Mit Richtlinien können Sie den Zeitplan für lokale Systemaufgaben auf allen geschützten Servern, die zur einen Gruppe gehören, ausschalten.

Allgemeine Informationen über den Aufgaben in Kaspersky Administration Kit stehen im Dokument *Kaspersky Administration Kit. Administratorhandbuch*.

21.2. Aufgabe erstellen

Um eine neue Aufgabe in der Administrationskonsole zu erstellen, machen Sie Folgendes:

1. Starten Sie den Assistenten für die Aufgabenerstellung:

   - *Für* eine *lokale Aufgabe*:

     a) Im Baum der Administrationskonsole klappen Sie den Knoten **Gruppen** auf und gehen auf die Gruppe, zu der der geschützte Server gehört.

     b) Im Ergebnisfenster öffnen Sie das Kontextmenü mit einem Rechtsklick auf die Zeile mit dem geschützten Server und gehen Sie auf **Eigenschaften**.

     c) Auf der Registerkarte **Aufgaben** klicken Sie auf die Schaltfläche **Hinzufügen**,

   - *Für das* Erstellen *einer Gruppenaufgabe*:

     a) in der Administrationskonsole wählen Sie die Gruppe, für die Sie eine Gruppenaufgabe erstellen wollen;

     b) Öffnen Sie das Kontextmenü für den eingebetteten Ordner **Gruppenaufgaben** und gehen Sie auf **Neu** → **Aufgabe**.

   - *Für das Erstellen einer globalen Aufgabe* öffnen Sie in der Administrationskonsole das Kontextmenü mit einem Rechtsklick auf den Knoten **Globale Aufgaben** und gehen Sie auf **Neu** → **Aufgabe**.

   Es öffnet sich das Begrüßungsfenster des Assistenten.

2. Im Fenster des Assistenten für die Aufgabenerstellung **Aufgabenname** geben Sie den Namen der Aufgabe an (nicht mehr als 100 Zeichen, kann keine Sonderzeichen символы **" * < > ? \ / | :)** enthalten). Wir empfehlen das Aufgabetyp in dem Namen anzugeben (z. B., «Untersuchung der gemeinsame Ordner»).

3. Im Fenster **Anwendungen** wählen Sie unter der Überschrift **Anwendung Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition** unter der Überschrift **Aufgabentyp** den Typ der zu erstellenden Aufgabe.

4. Je nach Typ der zu erstellenden Aufgabe führen Sie eine der folgenden Aktionen aus:

   - Wenn Sie eine Aufgabe zur Virensuche erstellen:

a) Im Fenster **Einstellungen** legen Sie den Untersuchungsbereich an.

Standardmäßig steht im Untersuchungsbereich der vordefinierten Bereich **Arbeitsplatz** (s. Abbildung 121).

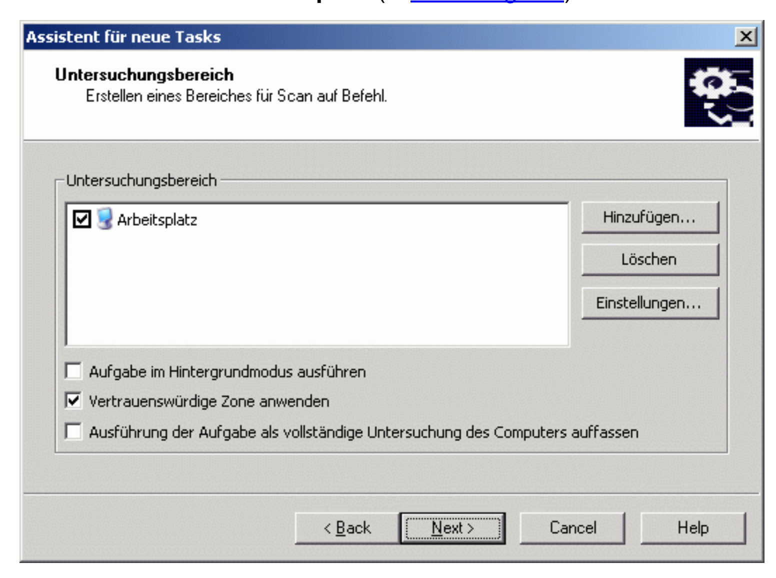


Abbildung 121. Fenster **Untersuchungsbereich** des Assistenten für die Aufgabenerstellung

Der Bereich **Arbeitsplatz** enthält eingebettete Bereiche, die in Abbildung 122 zu sehen sind. (Diese Bereiche sind in Pkt. 9.2.1.2 auf S. 125 beschrieben.)

Wenn es aus Sicherheitsgründen nicht erforderlich ist den kompletten Server zu untersuchen, dann kann der Untersuchungsbereich begrenzt werden: Es können nur einzelne vordefinierte Bereiche und/oder einzelne Datenträger, Ordner oder Dateien untersucht werden.

- Um einzelne Bereiche, Datenträger, Ordner oder Dateien zum Untersuchungsbereich hinzuzufügen, entfernen Sie im Dialogfenster **Einstellungen** den vordefinierten Bereich **Arbeitsplatz**. Danach klicken Sie auf die Schaltfläche **Hinzufügen**, im Dialogfenster **Zum Untersuchungsbereich hinzufügen** wählen Sie die Objekte, die in den Untersuchungsbereich hineinkommen sollen: Wählen Sie den vordefinierten Bereich aus der Liste **Vordefinierter Untersuchungsbereich** (s. Abbildung 122) aus, geben Sie den Datenträger des Server, den Ordner

oder die Datei auf dem Server oder auf einem anderen Computer im Netzwerk an und klicken Sie auf die Schaltfläche **OK**.

Zum Untersuchungsbereich hinzufügen
Vordefinierter Untersuchungsbereich:
Arbeitsplatz
Laufwerk oder Ordner:
Durchsuchen
Datei:
Durchsuchen
OK
Abbrechen

Abbildung 122. Dialogfenster **Zum Untersuchungsbereich hinzufügen**

- Um eingebettete Ordner oder Dateien von der Untersuchung auszuschließen, wählen Sie den hinzugefügten Ordner (Datenträger) im Fenster **Einstellungen** des Assistenten, klicken Sie auf die Schaltfläche **Einstellungen**, danach in dem Fenster E**instellungen zur Virensuche** klicken Sie auf die Schaltfläche **Einstellung** und im Dialogfenster **Einstellung des Schutzbereiches** nehmen Sie das Häkchen in **Eingebettete Ordner (Eingebettete Dateien)** heraus.

- Aktivieren Sie das Kontrollkästchen **Vertrauenswürdige Zone anwenden**, wenn Sie in der Aufgabe vom Schutzbereich diejenigen Objekte ausschließen wollen, die in der vertrauenswürdigen Zone des Anti-Virus beschrieben werden (Details zur vertrauenswürdigen Zone lesen Sie in Pkt. 8.1 auf S. 109; wie Ausnahmen in die vertrauenswürdige Zone im Programm Kaspersky Administration Kit aufgenommen werden, lesen Sie in Pkt. 20.7 auf S. 323).

b) Wenn Sie vorhaben, die zu erstellende Aufgabe als Vollständige Untersuchung des Computers zu benutzen, setzen Sie Häkchen in **Aufgabenausführung als vollständige Untersuchung des Servers betrachten**. Die Anwendung Kaspersky Administration Kit wird den Sicherheitszustand des Servers (der Server) nach den Ergebnissen der Aufgabe "Volle Computeruntersuchung" beurteilen, und nicht nach den Ergebnissen der Systemaufgabe **Untersuchung von Arbeitsplatz**. Details darüber, wie der Aufgabe zur Virensuche der Status "Aufgabe Vollständige Untersuchung des Computers" vergeben wird, finden Sie in Pkt. 21.4 auf S.346.

c) Um einem Arbeitsprozess, in dem eine Aufgabe ausgeführt wird, die Basispriorität **Niedrig** (**Low**) zuzuweisen, setzen Sie das Häkchen in **Aufgabe im Hintergrund ausführen**. In der Grundeinstellung haben Arbeitsprozesse, die Aufgaben des Anti-Virus ausführen, die Priorität **Mittel** (**Normal**). Das Senken der Priorität eines Prozesses verlängert die Aufgabenausführung und beeinflusst positiv das Tempo der Prozessausführung von anderen aktiven Anwendungen.

- Wenn Sie eine der Aufgaben zum Update erstellen, aktivieren Sie die gewünschten Aufgabenparameter nach Ihren Bedürfnissen:

  a) Wählen Sie eine Updatequelle im Fenster **Einstellungen** aus (s. Pkt. B.5.1 auf S. 419).

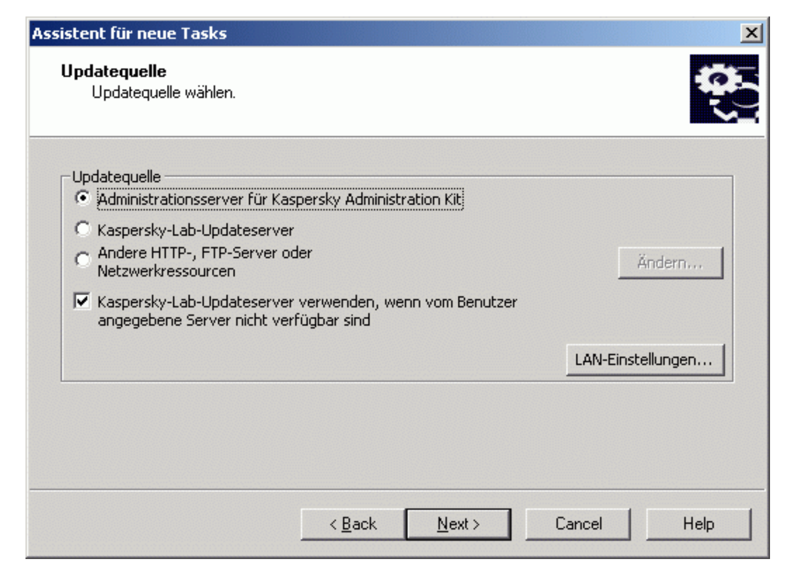


Abbildung 123. Fenster **Einstellungen**

  b) Klicken Sie auf die Schaltfläche **LAN-Einstellungen**. Es öffnet sich das Dialogfenster **Verbindungseinstellungen** (s. Abbildung 124).

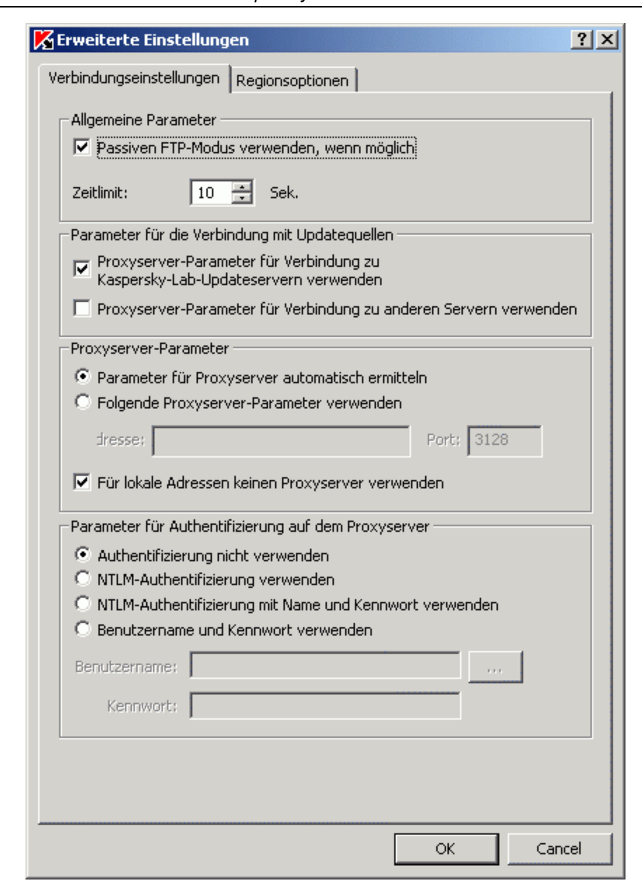


Abbildung 124. Dialogfenster **Erweiterte Einstellungen**, Registerkarte **Verbindungseinstellungen**

c) Auf der Registerkarte **Verbindungseinstellungen** führen Sie die folgenden Aktionen durch:

- Geben Sie den Modus des FTP-Servers für die Verbindung mit dem geschützten Server an (s. Pkt. B.5.2 auf S. 421).
- Bei Bedarf ändern Sie die Wartezeit für die Verbindung mit der Updatequelle (s. Pkt. B.5.3 auf S. 421).
- Stellen Sie die Zugangsparameter für den Proxy-Server während der Verbindung mit der Updatequelle ein (s. Pkt. B.5.4 auf S. 422).

d) Auf der Registerkarte **Regionsoptionen** wählen Sie die Lage des geschützten Servers (der Server) aus, um den Update-Download zu optimieren (s. Pkt. B.5.5 auf S. 425).

- Wenn Sie die Aufgabe ***Update der Programm-Module*** erstellen, stellen Sie im Fenster **Update-Einstellungen** (s. *Abbildung 125*) die gewünschten Parameter für das Update der Programm-Module ein:

  a) Wählen Sie, ob kritische Updates der Programm-Module heruntergeladen und installiert werden sollen, oder nur das Vorhandensein von Updates überprüft werden soll (s. Pkt. B.5.6.1 auf S. 426).

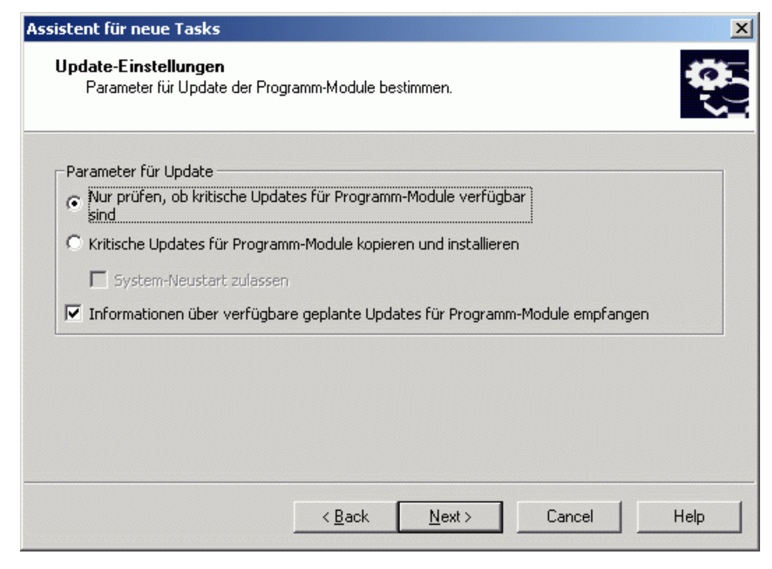


Abbildung 125. Fenster **Update-Einstellungen** in Aufgabe **Update der Programm-Module**

  b) Wenn Sie **Kritische Updates für Programm-Module kopieren und installieren** ausgewählt haben: um die Änderungen zu übernehmen kann ein Neustart notwendig sein. Um den Neustart des Servers zu erlauben, setzen Sie das Häkchen in **System-Neustart zulassen**. Um den Neustart des Servers zu verschieben, entfernen Sie das Häkchen in **System-Neustart zulassen**.

  c) Wenn Sie Informationen über geplante Modul-Updates erhalten wollen, setzen Sie Häkchen **Informationen über verfügbare geplante Updates für Programm-Module empfangen**.

"Kaspersky Lab" veröffentlicht keine geplanten Updates zum automatischen Updaten; Sie können diese selbst von der Internetseite von "Kaspersky Lab" laden. Sie können Benachrichtigung des Administrators über Ereignis *Neue geplante Modul-Updates des Anti-Virus sind verfügbar*, in welcher Internetadresse unseren Seite enthalten ist, woher die Updates geladen werden können (Details über die Einstellung der Benachrichtigung lesen Sie in Pkt. 15.2 auf S. 237).

- *Wenn Sie die Aufgabe **Update-Verteilung*** erstellen, geben Sie im Fenster **Parameter für Update-Verteilung einstellen** die Updates (s. Pkt. B.5.7.1 auf S. 428) und einen Ordner zum Speichern an (s. Pkt. B.5.7.2 auf S. 429).

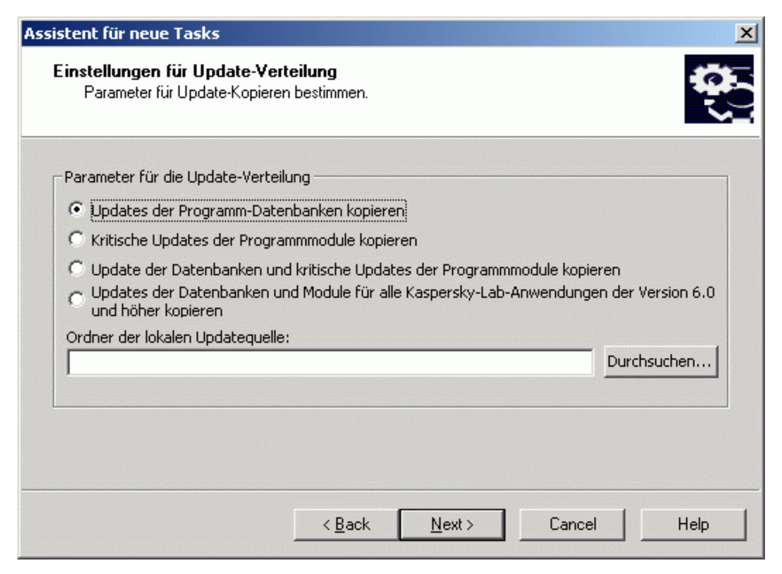


Abbildung 126. Fenster **Parameter für Update-Verteilung bestimmen**

- *Wenn Sie die Aufgabe **Lizenzschlüssel installieren*** erstellen, geben Sie im Fenster **Lizenzschlüssel installieren** (s. Abbildung 127) im Feld **Lizenzschlüssel** den Namen der Schlüsseldatei mit der Endung .key und den vollständigen Pfad zur Datei an.

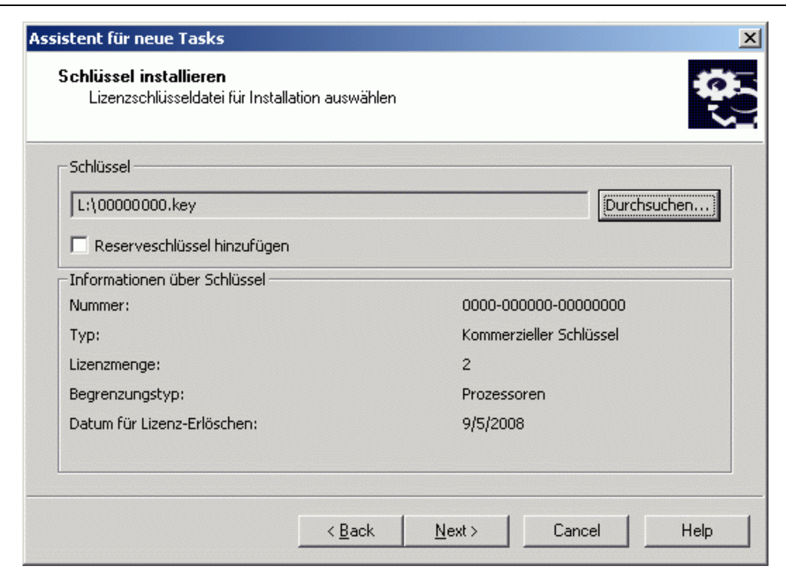


Abbildung 127. Fenster **Schlüssel installieren**

5. Stellen Sie die gewünschten Parameter für den Aufgabenzeitplan ein (Sie können den Aufgabenzeitplan für alle Aufgabetypen einstellen, außer für die Aufgaben **Schlüssel installieren** und **Rollback des Datenbank-Updates**). Im Fenster **Zeitplan** (s. Abbildung 128) führen Sie die folgenden Aktionen aus:

   a) Um den Zeitplan einzuschalten, setzen Sie das Häkchen in **Aufgabe nach Zeitplan starten**.

   b) Geben Sie die Starthäufigkeit an, mit der die Aufgabe gestartet wird (s. Pkt. B.2.1 auf S. 390): Wählen Sie aus der Liste **Startfrequenz** einen der folgenden Werte aus: **Stündlich**, **Täglich**, **Wöchentlich**, **Bei Programmstart**, **Nach dem Updaten** (in den Aufgaben **Anwendungsdatenbanken Updates**, **Anwendungsmodulen Update** und **Kopieren der Updates** können Sie die Häufigkeit des Startens **Nach Update-Download durch Administrationsserver** einstellen):

      - Wenn Sie **Stündlich** gewählt haben, geben Sie den Wert **Jede <Zahl> Stunde** in der Parametergruppe **Parameter für Aufgabenstart** an.

      - Wenn Sie **Täglich** gewählt haben, geben Sie die Anzahl der Tage im Feld **Alle <Zahl> Tage** in der Parametergruppe **Parameter für Aufgabenstart** an.

- Wenn Sie **Wöchentlich** gewählt haben, geben Sie die Anzahl der Wochen im Feld **Jede <Zahl> Woche** in der Parametergruppe **Parameter für Aufgabenstart** an. Legen Sie fest, an welchen Wochentagen die Aufgabe gestartet wird (standardmäßig wird eine Aufgabe montags gestartet).

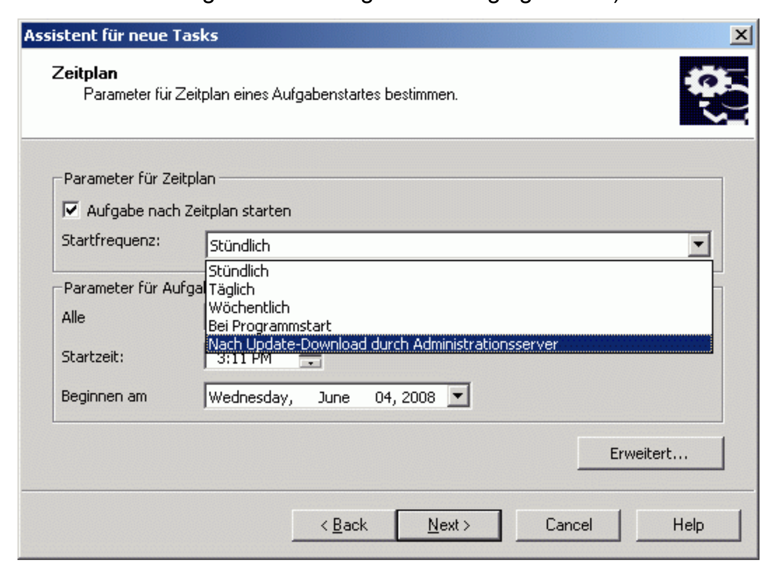


Abbildung 128. Beispiel des Fensters **Zeitplan**, Startfrequenz **Nach Update-Download durch Administrationsserver**

c) Im Feld **Startzeit** geben Sie die erste Startzeit der Aufgabe ein, in das Feld **Starten** geben Sie Datum, an dem der Zeitplan in Kraft tritt. (s. Pkt. B.2.2 auf S. 391)

d) Geben Sie bei Bedarf die übrigen Zeitplan-Parameter an: Klicken Sie auf die Schaltfläche **Erweitert** und führen Sie im Dialogfenster **Erweiterte Einstellungen für den Zeitplan** (s. Abbildung 129) die folgenden Aktionen aus:

- Geben Sie maximale Laufzeit der Aufgabe an: In der Gruppe **Parameter für das Anhalten der Aufgabe**, geben Sie im Feld **Dauer** geben Sie die gewünschte Anzahl der Stunden und Minuten an (s. Pkt. B.2.4 auf S. 393).

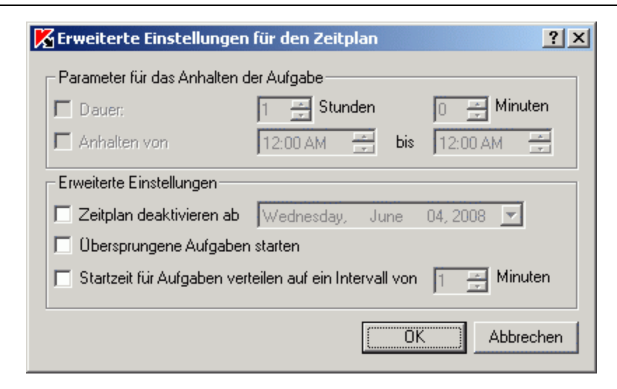


Abbildung 129. Dialogfenster **Erweiterte Einstellungen für den Zeitplan**

- Geben Sie die Zeitperiode innerhalb von 24 Stunden an, während derer das Ausführen der Aufgabe angehalten wird: In der Gruppe **Parameter für das Anhalten der Aufgabe** geben Sie in dem Feld **Anhalten von … bis** die Anfangs- und Endwerte an (s. Pkt. B.2.5 auf S. 393).
- Wählen Sie ein Datum, von dem an der Zeitplan nicht mehr gültig ist: Setzen Sie das Häkchen in **Zeitplan deaktivieren ab** und wählen Sie mit dem Dialogfenster **Kalender** das Datum, von dem an der Zeitplan nicht mehr gültig ist (s. Pkt. B.2.3 auf S. 392).
- Aktivieren Sie die Startfunktion für übersprungene Aufgaben: Setzen Sie das Häkchen in **Übersprungene Aufgaben starten** (s. Pkt. B.2.6 auf S. 394).
- Aktivieren Sie den Parameter **Startzeit-Verteilung**: Setzen Sie das Häkchen in **Startzeit für Aufgaben verteilen auf ein Intervall von** und geben Sie den Parameterwert in Minuten ein (s. Pkt. B.2.7 auf S. 395).

e) Klicken Sie auf **OK**.

6. Wenn die Aufgabe eine globale Aufgabe ist, wählen Sie die Netzwerkcomputer (Gruppen) aus, an denen die Aufgabe ausgeführt werden soll.
7. Im Fenster **Assistenten schließen** klicken Sie auf die Schaltfläche **Fertig**.

Die erstellte Aufgabe erscheint im Dialogfenster **Aufgaben**.

21.3. Aufgaben einstellen

Nachdem die Aufgabe erstellt wurde, können Sie folgende Einstellungen vornehmen:

- Aufgabenparameter ändern
- Aufgabenzeitplan einstellen / ändern
- Benutzerkonto auswählen, mit dessen Rechten die Aufgabe ausgeführt wird
- Benachrichtigungen über Aufgabenergebnisse einstellen

Um eine Aufgabe anzupassen:

1. In der Administrationskonsole klappen Sie den Knoten **Gruppen** auf und gehen auf die Gruppe, zu der der geschützte Server gehört.
2. In dem Ergebnisfenster öffnen Sie das Kontextmenü mit einem Rechtsklick auf die Zeile mit dem geschützten Server und gehen Sie auf **Eigenschaften**.
3. Im Dialogfenster E**igenschaften: <Computer>** öffnen Sie auf der Registerkarte **Aufgabe** das Kontextmenü mit einem Rechtsklick auf die Aufgabe, die Sie einstellen wollen, und gehen Sie auf **Eigenschaften**.
4. Passen Sie bei Bedarf die Aufgabenparameter an:
   - In der Aufgabe **Echtzeitschutz für Dateien** auf der Registerkarte **Anpassen**:

     Legen Sie den Schutzbereich fest (Informationen über vordefinierte Bereiche finden Sie in Pkt. 6.2.1.2 auf S. 73).

     Übernehmen Sie die vertrauenswürdige Zone: Klicken Sie auf die Schaltfläche **Schutzmodus** und aktivieren Sie im Dialogfenster **Erweitert** das Kontrollkästchen **Vertrauenswürdige Zone anwenden** (Informationen zum Anlegen der vertrauenswürdigen Zone siehe Pkt. 20.7.3 auf S. 327).

     Um den Schutzmodus für Objekte zu ändern, klicken Sie auf die Schaltfläche **Schutzmodus** und wählen Sie im Dialogfenster **Erweitert** den gewünschten Schutzmodus für Objekte (Details über diesen Parameter finden Sie in Pkt. B.3.1 auf S. 396).
   - In der Aufgabe **Skript-Untersuchung** auf der Registerkarte **Anpassen**:

Legen Sie fest, ob die Ausführung von Skripts, die Anti-Virus als verdächtig einstuft, erlaubt oder verboten werden soll.

Übernehmen Sie die vertrauenswürdige Zone (Informationen über das Anlegen der vertrauenswürdigen Zone s. Pkt. 20.7.3 auf S. 327).

- In der Aufgabe **Vollständige Untersuchung des Computers** auf der Registerkarte **Untersuchungsbereich**:

  Legen Sie den Schutzbereich fest (Informationen über vordefinierte Bereiche finden Sie in Pkt. 9.2.1.2 auf S. 125).

  Ändern Sie die Priorität des aktiven Prozesses, in dem die Aufgabe ausgeführt werden soll (s. Pkt. 9.3 auf S. 143).

  Weisen Sie der Aufgabe den Status "Aufgabe zur vollständigen Untersuchung des Computers" zu (s. Pkt. 21.4 auf S. 346).

  Übernehmen Sie die vertrauenswürdige Zone (Informationen zum Anlegen der vertrauenswürdigen Zone siehe Pkt. 20.7.3 auf S. 327).

- In der Aufgabe **Update-Verteilung**:

  Legen Sie auf der Registerkarte zum **Anpassen der Update-Verteilung** die Zusammensetzung der Updates und den Ordner zum Speichern fest (s. Pkt. B.5.7 auf S. 428).

  Geben Sie auf der Registerkarte **Updatequelle** die Updatequelle an (s. Pkt. B.5.1 auf S. 419).

- Auf der Registerkarte **Zeitplan** stellen Sie den Zeitplan für Aufgaben ein (s. Pkt. 5 der Anweisungen für die Aufgabenerstellung auf S. 341).

- Auf der Registerkarte **Benutzerkonto** wählen Sie das Benutzerkonto, mit dessen Berechtigungen die Aufgabe ausgeführt wird (s. Pkt. 5.9.1 auf S. 65).

- Auf der Registerkarte **Benachrichtigung** stellen Sie die Benachrichtigung über die Ergebnisse der Aufgabenausführung ein (Details finden Sie im Dokument *Kaspersky Administration Kit. Benutzerhandbuch*).

> **Anmerkung**
>
> Gilt eine Richtlinie von Kaspersky Administration Kit, lassen sich Parameterwerte, die in der Richtlinie mit dem Symbol 🔒 im Dialogfenster **Eigenschaften der Aufgabe** der Administrationskonsole gekennzeichnet sind, sind ändern.

5. Klicken Sie auf die Schaltfläche **OK**.
6. Klicken Sie auf **OK** im Dialogfenster **Eigenschaften der Aufgabe**, um die Änderungen zu speichern.

21.4. Vollständige Untersuchung der Server verwalten in Zuweisen des Status *Aufgabe Vollständige Untersuchung des Computers* an eine Aufgabe zur Virensuche

In der Grundeinstellung weist Kaspersky Administration Kit dem Server den Status *Warnung* zu, wenn die Aufgabe **Vollständige Untersuchung des Computers** eher ausgeführt wird, als im Anti-Virus-Parameter **Grenzwert für Eintritt des Ereignisses *Vollständige Untersuchung des Servers liegt lange zurück*** angegeben ist.

Sie können die vollständige Untersuchung aller Server, die zu einer Administrationsgruppe gehören, auf folgende Weise gleichzeitig "verwalten":

1. Erstellen Sie eine Gruppenaufgabe zur Virensuche. Im Fenster **Einstellungen** des Assistenten für die Aufgabenerstellung weisen Sie ihr den Status "Aufgabe Vollständige Untersuchung des Computers" zu. Die von Ihnen angegebenen Aufgabenparameter, nämlich der Untersuchungsbereich und die Parameter für Sicherheit, sind für alle Server der Gruppe gleich. Stellen Sie einen Aufgabenzeitplan ein. Details dazu, wie eine Aufgabe erstellt wird, finden Sie in Pkt. 21.2 auf S. 334.

> **Anmerkung**
>
> Sie können einer Aufgabe zur Virensuche den Status "Aufgabe Vollständige Untersuchung des Computers" beim Erstellen oder später im Dialogfenster **Aufgabeneigenschaften** zuweisen.

2. Mit einer neuen oder vorhandenen Richtlinie deaktivieren Sie die Systemaufgabe **Vollständige Untersuchung des Computers** auf den Servern der Gruppe (s. Pkt. 19.4 auf S. 297).

Von diesem Zeitpunkt an berücksichtigt der Administrationsserver von Kaspersky Administration Kit bei der Bewertung des Sicherheitszustands des geschützten Servers und bei der Benachrichtigung darüber die Ergebnisse der letzten Aufgabenausführung mit dem Status "Aufgabe zur vollständigen Untersuchung des Computers", nicht die Ausführungsergebnisse der Systemaufgabe **Vollständige Untersuchung des Computers**.

Sie können den Status "Aufgabe Vollständige Untersuchung des Computers" nicht nur Gruppenaufgaben, sondern auch lokalen und globalen Aufgaben zur Virensuche zuweisen.

In der Anti-Virus-Konsole in der MMC können Sie überprüfen, ob Gruppenaufgaben oder globalen Aufgaben zur Virensuche als Aufgabe Vollständige Untersuchung des Computers betrachtet werden.

> **Anmerkung**
>
> In der Anti-Virus-Konsole wird das Häkchen in **Ausführung der Aufgabe als vollständige Untersuchung des Computers auffassen** in den Aufgabeneigenschaften nur angezeigt und kann nicht geändert werden.

TEIL 4. ANTI-VIRUS-COUNTER

In diesem Abschnitt stehen die folgenden Informationen:

- Beschreibung von Produktivitäts-Countern für die Anwendung System-Monitor (s. Kapitel 22 auf S. 349)
- Beschreibung der SNMP-Counter und -Schwachstellen für Anti-Virus (s. Kapitel 23 auf S. 359)

KAPITEL 22. PRODUKTIVITÄTS-COUNTER FÜR ANWENDUNG "SYSTEMMONITOR"

In diesem Kapitel stehen allgemeine Informationen über die Produktivitäts-Counter des Anti-Virus (s. Pkt. 22.1 auf S. 349) und jeder Counter wird näher beschrieben:

- Summe der abgelehnten Anfragen (s. Pkt. 22.2 auf S. 350)
- Summe der übersprungenen Anfragen (s. Pkt. 22.3 auf S. 351)
- Summe der Anfragen, die wegen ungenügender Systemressourcen nicht verarbeitet wurden (s. Pkt. 22.4 auf S. 352)
- Summe der Anfragen, die zur Verarbeitung weitergeleitet wurden (s. Pkt. 22.5 auf S. 353)
- Mittelwert der Datenströme vom File-Interception-Dispatcher (s. Pkt. 22.6 auf S. 354)
- Höchstwert der Datenströme vom File-Interception-Dispatcher (s. Pkt. 22.7 auf S. 355)
- Summe der infizierten Objekte in Warteschlange für Verarbeitung (s. Pkt. 22.8 auf S. 356)
- Summe der Objekte, die pro Sekunde verarbeitet werden (s. Pkt. 22.9 auf S. 357)

22.1. Produktivitäts-Counter des Anti-Virus

Wenn als zu installierende Anti-Virus-Komponenten die Komponente **Produktivitäts-Counter** aktiviert worden ist, registriert Anti-Virus während der Installation seine Produktivitäts-Counter für die Anwendung System-Monitor von Microsoft Windows.

Mit den Anti-Virus-Countern können Sie die Produktivität des Anti-Virus bei der Ausführung der Aufgabe Echtzeitschutz kontrollieren. Sie können Engstellen beim Zusammenwirken mit anderen Anwendungen und bei ungenügenden Ressourcen überwachen. Außerdem können Sie nicht so optimale Einstellungen des Anti-Virus und Abstürze diagnostizieren.

Sie können die Produktivitäts-Counter des Anti-Virus anzeigen, indem Sie die Konsole **Leistung** im Element des Verwaltungsfensters **Administration** öffnen.

Die folgenden Punkte erklären die Counter, nennen die empfohlenen Intervalle für das Ablesen der Werte und entsprechende Grenzwerte. Außerdem werden Empfehlungen zur Konfiguration von Anti-Virus bei Grenzwertüberschreitungen gegeben.

22.2. Summe der abgelehnten Anfragen

Name	Summe der abgelehnten Anfragen (Number of requests denied)
Bestimmung	Summe der Anfragen von File-Interceptor-Treiber für die Objektverarbeitung, die nicht von Anti-Virus-Prozessen angenommen wurden; gezählt ab dem letzten Anti-Virus-Start. Anti-Virus überspringt Objekte, deren Verarbeitungsanfragen von aktiven Anti-Virus-Prozessen zurückgewiesen werden.
Ziel	Ein Counter kann überwachen: • Qualitätsverluste beim Echtzeitschutz wegen hoher Belastung der Anti-Virus-Prozesse • Unterbrechung des Echtzeitschutzes wegen Abweisungen vom File-Interception-Dispatcher
Normalwert / Schwellenwert	0 / 1
Empfohlenes Intervall zum Ablesen der Werte	1 Stunde
Empfehlungen für Einstellung, wenn	Summe der abgelehnten Anfragen für die Verarbeitung entspricht der Summe der übersprungenen Objekte

Counter-Wert Schwellenwert überschreitet	Mögliche folgende Situationen je nach "Verhalten" des Counters: • Counter zeigt mehrere abgelehnte Anfrage im Laufe einer längeren Zeit: Alle Anti-Virus-Prozesse wurden vollständig geladen, darum konnte Anti-Virus die Objekte nicht untersuchen. Um das Überspringen von Objekten auszuschließen, erhöhen Sie die Menge an Anti-Virus-Prozessen für Aufgaben des Echtzeitschutzes. Sie können die Anti-Virus-Parameter **Maximale Anzahl der Arbeitsprozesse** (Details zum Parameter finden Sie in Pkt. B.1.1 auf S. 376) und **Anzahl der Prozesse für den Echtzeitschutz** (Details zum Parameter finden Sie in Pkt. B.1.2 auf S. 377) nutzen. • Die Summe der abgelehnten Anfragen übersteigt den kritischen Schwellenwert erheblich und steigt schnell an: Der File-Interception-Dispatcher ist ausgefallen. Anti-Virus untersucht keine Objekte beim Zugriff. Starten Sie Anti-Virus noch einmal.

22.3. Summe der übersprungenen Anfragen

Name	Summe der übersprungenen Anfragen (Number of requests skipped)
Bestimmung	Summe der Anfragen des File-Interception-Treibers für die Verarbeitung von Objekten, die vom Treiber-Prozess angenommen wurden, für die aber keine Ereignisse über den Verarbeitungsabschluss geschickt wurden; gezählt ab dem letzten Anti-Virus-Start. Wenn eine Anfrage zur Verarbeitung eines Objekts, das von einem aktiven Prozess angenommen wurde, kein Ereignis über den Verarbeitungsabschluss geschickt hat, übergibt der Treiber diese Anfrage an einen anderen Prozess und der Wert des Counters **Summe der übersprungenen Anfragen** wird um 1 erhöht. Wenn der Treiber alle aktiven Prozesse aufgerufen hat und die Verarbeitungsanfrage von keinem der Prozesse angenommen wurde (wegen Beschäftigung) oder keine Ereignisse über den Verarbeitungsabschluss gesendet wurden, überspringt Anti-Virus

	das Objekt und erhöht den Wert des Counters **Summe der übersprungenen Anfragen** um 1.
Ziel	Der Counter kann einen Produktivitätsverlust wegen ausbleibender Datenströme vom File-Interception-Dispatcher überwachen.
Normalwert / Schwellenwert	0 / 1
Empfohlenes Intervall zum Ablesen der Werte	1 Stunde
Empfehlungen für Einstellung, wenn Counter-Wert Schwellenwert überschreitet	Ein Counter-Wert, der ungleich Null ist, bedeutet, dass ein oder mehrere Datenströme des File-Interception-Dispatchers hängen geblieben sind und stillstehen. Der Counter-Wert entspricht den Anzahl der Datenströme, die zurzeit stillstehen. Wenn das Untersuchungstempo nicht befriedigt, starten Sie Anti-Virus noch einmal, um die angehaltenen Datenströme wiederherzustellen.

22.4. Anzahl der Anfragen, die wegen ungenügender Systemressourcen nicht verarbeitet wurden

Name	Summe der Anfragen, die aufgrund nicht genügender Systemressourcen nicht verarbeitet wurden (Number of requests not processed due to lack of resources)
Bestimmung	Summe der Anfragen des File-Interception-Treibers, die aufgrund ungenügender Systemressourcen (beispielsweise Arbeitsspeicher) nicht verarbeitet wurden; gezählt ab dem letzten Anti-Virus-Start. Anti-Virus überspringt Objekte, deren Verarbeitungsanfragen von den aktiven Anti-Virus-Prozessen zurückgewiesen werden.

Ziel	Der Counter kann mögliche Qualitätsverluste des Echtzeitschutzes erkennen und beseitigen, die aufgrund nicht genügender Systemressourcen eintreten.
Normalwert / Schwellenwert	0 / 1
Empfohlenes Intervall zum Ablesen der Werte	1 Stunde
Empfehlungen für Einstellung, wenn Counter-Wert Schwellenwert überschreitet	Wenn der Counter-Wert ungleich Null ist, brauchen die Anti-Virus-Prozesse für die Anfragenbearbeitung einen größeren Arbeitsspeicher. Es ist möglich, dass es andere Prozesse gibt, die den ganzen Arbeitsspeicher in Anspruch nehmen.

22.5. Summe der Anfragen, die zur Verarbeitung weitergeleitet wurden

Name	Summe der Anfragen, zur Verarbeitung weitergeleitet wurden (Nummer of requests sent to be processed)
Bestimmung	Summe der Objekte, die zurzeit auf Verarbeitung durch die Arbeitsprozesse warten
Ziel	Der Counter kann das Laden der Anti-Virus-Prozesse und das Niveau der Dateiaktivität auf dem Server verlangsamen.
Normalwert / Schwellenwert	Der Counter-Wert kann schwanken, je nach Niveau der Dateiaktivität auf dem Server.
Empfohlenes Intervall zum Ablesen der Werte	1 Min.

Empfehlungen für Einstellung, wenn Counter-Wert Schwellenwert überschreitet	Nein

22.6. Mittelwert der Datenströme vom File-Interception-Dispatcher

Name	Mittelwert der Datenströme vom File-Interception-Dispatcher (Average number of file interception dispatcher streams)
Bestimmung	Anzahl der Datenströme vom File-Interception-Dispatcher in einem Prozess, der von allen Prozess im Mittelfeld liegt, der von den Aufgaben des Echtzeitschutzes zurzeit belegt ist
Ziel	Der Counter kann mögliche Qualitätsverluste des Echtzeitschutzes erkennen und beseitigen, die aufgrund eines nicht kompletten Ladens der Anti-Virus-Prozesse eintreten.
Normalwert / Schwellenwert	variiert / 40
Empfohlenes Intervall zum Ablesen der Werte	1 Min.

Empfehlungen für Einstellung, wenn Counter-Wert Schwellen-wert überschreitet	In jedem Arbeitsprozess können bis zu 60 Datenströme des File-Interception-Dispatchers angelegt werden. Wenn sich der Counter-Wert der Zahl 60 nähert, besteht das Risiko, dass kein Arbeitsprozess mehr die Verarbeitung einer in der Warteschlange stehenden Anfrage vom File-Interception-Treiber abnimmt und Anti-Virus überspringt das Objekt. Vergrößern Sie die Anzahl der Anti-Virus-Prozesse für die Aufgaben des Echtzeitschutzes. Sie können die Anti-Virus-Parameter **Maximale Anzahl aktiver Prozesse** (Details zum Parameter finden Sie in Pkt. B.1.1 auf S. 376) und **Anzahl der Prozesse für den Echtzeitschutz** (Details zum Parameter finden Sie in Pkt. B.1.2 auf S. 377) nutzen.

22.7. Höchstwert der Datenströme vom File-Interception-Dispatcher

Name	Höchstwert der Datenströme vom File-Interception-Dispatcher (Maximum number of file interception dispatcher streams)
Bestimmung	Anzahl der Datenströme vom File-Interception-Dispatcher in einem Arbeitsprozess, der am meisten von allen Prozessen von den Aufgaben des Echtzeitschutzes zurzeit belegt ist
Ziel	Der Counter kann einen Produktivitätsverlust wegen ungleichmäßiger Belastungsverteilung in den ausgeführten Arbeitsprozessen erkennen und beseitigen.
Normalwert / Schwellenwert	variiert / 40
Empfohlenes Intervall zum Ablesen der Werte	1 Min.

Empfehlungen für Einstellung, wenn Counter-Wert Schwellenwert überschreitet	Wenn der Wert dieses Counters dauerhaft und erheblich vom Counter-Wert **Mittelwert der Datenströme vom File-Interception-Dispatcher** abweicht, verteilt Anti-Virus die Belastung ungleichmäßig auf die ausführenden Prozesse. Starten Sie Anti-Virus noch einmal.

22.8. Summe der infizierten Objekte in Warteschlange für Verarbeitung

Name	Summe der infizierten Objekte in Warteschlange für Verarbeitung (Number of items in the infected object queue)
Bestimmung	Summe der infizierten Objekte, die zurzeit auf Verarbeitung (Desinfektion oder Löschen) warten
Ziel	Ein Counter kann überwachen: • Unterbrechung des Echtzeitschutzes wegen möglichen Abweisungen vom File-Interception-Dispatcher • Überlastung des Prozessors wegen ungleichmäßiger Verteilung der Prozessorzeit zwischen den anderen laufenden Anwendungen und Anti-Virus • Virenepidemie
Normalwert / Schwellenwert	Der Counter-Wert kann von Null abweichen, wenn Anti-Virus gefundene infizierte oder verdächtige Objekt verarbeitet, aber nicht sofort nach Bearbeitungsschluss zur Null zurückkehrt. / Der Counter-Wert bleibt längere Zeit nicht auf Null.
Empfohlenes Intervall zum Ablesen der Werte	1 Min.
Empfehlungen für Einstellung, wenn Counter-Wert Schwellenwert überschreitet	Wenn der Counter-Wert längere Zeit nicht auf Null bleibt: • Anti-Virus verarbeitet keine Objekte (möglicherweise hat ihn der File-Interception-Dispatcher abgewiesen) Starten Sie Anti-Virus noch einmal.

	• Es steht nicht genügend Prozessorzeit für die Objektverarbeitung zur Verfügung. Räumen Sie Anti-Virus zusätzliche Prozessorzeit ein, indem Sie beispielsweise die Serverbelastung durch andere Anwendungen senken. • Es ist eine Virenepidemie eingetreten. Sie können die Funktion *Virenepidemien verhindern* aktivieren (s. Pkt. 7.5 auf S. 102). Vom Eintreten einer Virenepidemie zeugt außerdem eine große Menge an gefundenen infizierten oder verdächtigen Objekten in der Aufgabe **Echtzeitschutz für Dateien**. Sie können Informationen über die Menge der gefundenen Objekte in der Aufgabenstatistik (s. Pkt. 6.3 auf S. 91) oder im Detailbericht über die Aufgabenausführung (s. Pkt. 13.2.4 auf S. 210) anzeigen.

22.9. Summe der Objekte, die pro Sekunde verarbeitet werden

Name	Summe der Objekte, die pro Sekunde verarbeitet werden (Number of objects processed per second)
Bestimmung	Summe der verarbeiteten Objekte, geteilt durch die Zeit, in der dieses Objekte verarbeitet worden sind; in gleich großen Zeitabschnitten errechnet
Ziel	Der Counter widerspiegelt das Tempo der Objektverarbeitung. So können Produktivitätsverluste des Servers erkannt und beseitigt werden, die wegen schlecht verteilter Prozessorzeit an Arbeitsprozesse oder wegen eines Anti-Virus-Absturzes eingetreten sind.
Normalwert / Schwellenwert	variiert / nein
Empfohlenes Intervall zum Ablesen der Werte	1 Min.
Empfehlungen für	Die Counter-Werte hängen von den aktivierten Werten der

Einstellung, wenn Counter-Wert Schwellenwert überschreitet	Anti-Virus-Parameter und von der Belastung des Servers durch Prozesse anderer Anwendungen ab. Beobachten Sie längere Zeit das mittlere Anzeige-Niveau des Counters. Wenn das allgemeine Anzeige-Niveau gesunken ist: • Den Anti-Virus-Prozessen steht nicht genügend Prozessorzeit für die Objektverarbeitung zur Verfügung. Räumen Sie Anti-Virus zusätzliche Prozessorzeit ein, indem Sie beispielsweise die Serverbelastung durch andere Anwendungen senken. • Anti-Virus ist abgestürzt (mehrere Datenströme stehen still). Starten Sie Anti-Virus noch einmal.

KAPITEL 23. SNMP-COUNTER UND -SCHWACHSTELLEN FÜR ANTI-VIRUS

In diesem Kapitel stehen die folgenden Informationen:

- SNMP-Counter und -Schwachstellen des Anti-Virus (s. Pkt. 23.1 auf S. 359)
- Beschreibung von SNMP-Countern (s. Pkt. 23.2 auf S. 359)
- Beschreibung von SNMP-Schwachstellen (s. Pkt. 23.2.8 auf S. 364)

23.1. SNMP-Counter und –Schwachstellen für Anti-Virus

Wenn Sie als zu installierende Anti-Virus-Komponente die Komponente **SNMP-Counter und -Schwachstellen** aktiviert haben, können Sie Counter und Schwachstellen des Anti-Virus mit den Protokollen Simple Network Management Protocol (SNMP) und HP Open View anzeigen.

Um die Counter und Schwachstellen des Anti-Virus vom Desktop-Rechner des Administrators anzuzeigen, starten Sie auf dem geschützten Server den SNMP-Dienst (SNMP Service) und auf dem Administrator-Arbeitsplatz den SNMP-Dienst (SNMP Service) sowie den Dienst SNMP-Schwachstellen (SNMP Trap Service).

23.2. SNMP-Counter des Anti-Virus

Im Anti-Virus sind die folgenden SNMP-Counter vorgesehen:

- Produktivitäts-Counter (s. Pkt. 23.2.1 auf S. 360)
- allgemeine Counter (s. Pkt. 23.2.2 auf S. 360)
- Update-Counter (s. Pkt. 23.2.3 auf S. 361)
- Counter für Echtzeitschutz (s. Pkt. 23.2.4 auf S. 361)
- Counter für Quarantäne (s. Pkt. 23.2.5 auf S. 363)

- Counter für Backup (s. Pkt. 23.2.6 auf S. 363)
- Counter für Zugriffssperre von Computern auf den geschützten Server (s. Pkt. 23.2.7 auf S. 363)
- Counter für die Skript-Untersuchung (s. Pkt. 23.2.8 auf S. 364).

23.2.1. Produktivitäts-Counter

Counter	Bestimmung
currentRequestsAmount	Summe der Anfragen, die zur Verarbeitung weitergeleitet wurden (s. Beschreibung in Pkt. 22.5 auf S. 353)
currentInfectedQueueLength	Summe der infizierten Objekte in Warteschlange für Verarbeitung (s. Beschreibung in Pkt. 22.8 auf S. 356)
currentObjectProcessingRate	Summe der Objekte, die pro Sekunde verarbeitet werden (s. Beschreibung in Pkt. 22.9 auf S. 357)
currentWorkProcessesAmount	Summe der zurzeit laufenden Anti-Virus-Arbeitsprozesse

23.2.2. Allgemeine Counter

Counter	Bestimmung
currentApplicationUptime	Laufzeit des Anti-Virus seit dem letzten Start, in Hundertstel-Sekunden
currentFileMonitorTaskStatus	Status der Aufgabe **Echtzeitschutz für Dateien**: On – läuft; Off – beendet oder angehalten
currentScriptCheckerTaskStatus	Status der Aufgabe **Skript-Untersuchung**: On – läuft; Off – beendet oder angehalten

Counter	Bestimmung
lastFullScanAge	"Alter" der vergangenen vollständigen Serveruntersuchung (Zeitabschnitt in Sekunden zwischen Datum der Beendigung einer Aufgabe, die den Status *Aufgabe Vollständige Untersuchung des Computers* hat, und dem heutigen Tag)
licenseExpirationDate	Ablaufdatum für die Gültigkeit des Schlüssels (Wenn ein aktiver und ein Reserveschlüssel installiert sind, informiert das Datum darüber, wann die summierte Gültigkeitsdauer des aktiven und des Reserveschlüssels abläuft.)

23.2.3. Update-Counter

Counter	Bestimmung
avBasesAge	"Alter" der Datenbanken (Zeitabschnitt in Hundertstel-Sekunden zwischen Erstellungsdatum der zuletzt installierten Updates der Datenbanken und dem heutigen Tag)

23.2.4. Counter für Echtzeitschutz

Counter	Bestimmung
totalObjectsProcessed	Summe der untersuchten Objekte seit dem letzten Start der Aufgabe **Echtzeitschutz für Dateien**
totalInfectedObjectsFound	Summe der gefundenen infizierten Objekte seit dem letzten Start der Aufgabe **Echtzeitschutz für Dateien**
totalSuspiciousObjectsFound	Summe der gefundenen verdächtigen Objekte seit dem letzten Start der Aufgabe **Echtzeitschutz für Dateien**

Counter	Bestimmung
totalVirusesFound	Summe der gefundenen Bedrohungen seit dem letzten Start der Aufgabe **Echtzeitschutz für Dateien**
totalObjectsQuarantined	Summe der infizierten oder verdächtigen Objekte, die Anti-Virus in die Quarantäne verschoben hat; wird seit dem letzten Start der Aufgabe **Echtzeitschutz für Dateien** berechnet
totalObjectsNotQuarantined	Summe der der infizierten oder verdächtigen Objekte, die Anti-Virus versucht hat, vergeblich in die Quarantäne zu verschieben; wird seit dem letzten Start der Aufgabe **Echtzeitschutz für Dateien** berechnet
totalObjectsDisinfected	Summe der infizierten oder verdächtigen Objekte, die Anti-Virus desinfiziert hat, wird seit dem letzten Start der Aufgabe **Echtzeitschutz für Dateien** berechnet
totalObjectsNotDisinfected	Summe der infizierten oder verdächtigen Objekte, die Anti-Virus vergeblich versucht hat zu desinfizieren; wird seit dem letzten Start der Aufgabe **Echtzeitschutz für Dateien** berechnet
totalObjectsDeleted	Summe der infizierten oder verdächtigen Objekte, die Anti-Virus gelöscht hat; wird seit dem letzten Start der Aufgabe **Echtzeitschutz für Dateien** berechnet
totalObjectsNotDeleted	Summe der infizierten oder verdächtigen Objekte, die nicht gelöscht wurden; wird seit dem letzten Start der Aufgabe **Echtzeitschutz für Dateien** berechnet
totalObjectsBackedUp	Summe der infizierten oder verdächtigen Objekte, die Anti-Virus in den Backup verschoben hat; wird seit dem letzten Start der Aufgabe **Echtzeitschutz für Dateien** berechnet

Counter	Bestimmung
totalObjectsNotBackedUp	Summe der infizierten oder verdächtigen Objekte, die Anti-Virus versucht hat, vergeblich in den Backup zu verschieben; wird seit dem letzten Start der Aufgabe **Echtzeitschutz für Dateien** berechnet

23.2.5. Counter für Quarantäne

Counter	Bestimmung
totalObjects	Summe der Objekte im Quarantäne-Ordner
totalSuspiciousObjects	Summe der verdächtigen Objekte im Quarantäne-Ordner
currentStorageSize	Datenvolumen im Quarantäne-Ordner (MB)

23.2.6. Counter für Backup

Counter	Bestimmung
currentBackupStorageSize	Datenvolumen im Backup-Ordner (MB)

23.2.7. Counter für Zugriffssperre von Computern auf Server

Counter	Bestimmung
currentHostsBlocked	Menge der Computer in Sperrliste
totalNotBlocked	Summe der nicht ausgeführten Zugriffssperren von Computern, die von der Sperre ausgeschlossen sind (vertrauenswürdige Computer) seit Aktivierung der Funktion automatische Sperre

23.2.8. Counter für die Skript-Untersuchung

Counter	Erklärung
totalScriptsProcessed	Gesamtzahl der untersuchten Skripts
totalInfectedIDangerous-ScriptsFound	Gesamtzahl der gefundenen infizierten Skripts
totalSuspiciousScriptsFound	Gesamtzahl der gefundenen verdächtigen Skripts
totalScriptsBlocked	Gesamtzahl der Skripts, auf die der Zugriff blockiert wurde.

23.3. SNMP-Schwachstellen

In der folgenden Tabelle sind die SNMP-Schwachstellen des Anti-Virus beschrieben.

Schwachstelle	Beschreibung	Parameter
eventThreatDetected	Bedrohung erkannt Details dazu, wie Anti-Virus infizierte und verdächtige Objekte erkennt, finden Sie in Pkt. 1.1.3 auf S. 19.	eventDateAndTime eventSeverity computerName userName objectName threatName detectType detectCertainty
eventBackupStorageSizeExceeds	Maximale Größe des Backups ist erreicht. Das Datenvolumen im Backup-Ordner hat den Wert überschritten, der im Parameter **Maximale Größe des Backups** angegeben ist. Anti-Virus reserviert weiter infizierte Objekte.	eventDateAndTime eventSeverity eventSource

Schwachstelle	Beschreibung	Parameter
eventThresholdBackupS-torageSizeExceeds	Grenzwert für freien Speicherplatz im Backup erreicht. Die Größe des freien Speicherplatzes im Backup-Ordner, die im Parameter **Grenzwert für freien Speicherplatz im Backup** eingegeben wurde, ist auf den angegebenen Wert gesunken. Anti-Virus reserviert weiter infizierte Objekte.	eventDateAndTime eventSeverity eventSource
eventQuarantineStorage-SizeExceeds	Maximale Größe der Quarantäne ist erreicht Das Datenvolumen im Quarantäne-Ordner hat den Wert überschritten, der im Parameter **Maximale Größe der Quarantäne** angegeben ist. Anti-Virus verschiebt weiter verdächtige Objekte in die Quarantäne.	eventDateAndTime eventSeverity eventSource
eventThresholdQuaranti-neStorageSizeExceeds	Grenzwert für freien Speicherplatz in der Quarantäne erreicht. Die Größe des freien Speicherplatzes im Quarantäne-Ordner, die mit dem Parameter **Grenzwert für freien Speicherplatz in Quarantäne** eingegeben wurde, ist auf den angegebenen Wert gesunken. Anti-Virus verschiebt weiter verdächtige Objekte in die Quarantäne.	eventDateAndTime eventSeverity eventSource

Schwachstelle	Beschreibung	Parameter
eventObjectNotQuaranti-ned	Fehler beim Verschieben des Objekts in die Quarantäne	eventSeverity eventDateAndTime eventSource userName computerName objectName storageObjectNo-tAddedEventRea-son
eventObjectNotBackuped	Fehler beim Speichern einer Kopie des Objekts im Ba-ckup-Speicher	eventSeverity eventDateAndTime eventSource objectName userName computerName storageObjectNo-tAddedEventRea-son
eventQuarantineInterna-lError	Es ist ein Fehler mit der Qua-rantäne aufgetreten.	eventSeverity eventDateAndTime eventSource eventReason
eventBackupInternalError	Es ist ein Fehler mit dem Backup aufgetreten.	eventSeverity eventDateAndTime eventSource eventReason
eventAVBasesOutdated	Datenbanken sind veraltet. Es werden die Tage errech-net, die seit dem letzten Be-enden der Aufgabe Update der Datenbanken vergangen sind (lokale, Gruppen oder globale Aufgabe).	eventSeverity eventDateAndTime eventSource days

Schwachstelle	Beschreibung	Parameter
eventAVBasesTotallyOut-dated	Datenbanken sind stark ver-altet. Es werden die Tage errechnet, die seit dem letz-ten Beenden der Aufgabe Update der Datenbanken vergangen sind (lokale, Gruppen oder globale Auf-gabe).	eventSeverity eventDateAndTime eventSource days
eventApplicationModule-sIntegrityFailed	Es ist ein Fehler bei Prüfen Integrität der Programm-Module eingetreten.	eventSeverity eventDateAndTime eventSource
eventApplicationStarted	Anti-Virus läuft.	eventSeverity eventDateAndTime eventSource
eventApplicationShutdown	Anti-Virus ist beendet.	eventSeverity eventDateAndTime eventSource
eventFullScanWasntPer-formForALongTime	Eine vollständige Untersu-chung des Computers liegt lange zurück. Es werden die Tage seit dem letzten Ab-schluss der Aufgabe gezählt, die den Status *Aufgabe Voll-ständige Untersuchung des Computers* besaß.	eventSeverity eventDateAndTime eventSource days
eventLicenseHasExpired	Die Gültigkeitsdauer des Lizenzschlüssels ist abgelau-fen.	eventSeverity eventDateAndTime eventSource
eventLicenseExpiresSoon	Die Gültigkeitsdauer des Lizenzschlüssels läuft bald ab. Es werden die Tage be-rechnet, die bis zum Ablauf der Gültigkeitsdauer für den Lizenzschlüssel bleiben.	eventSeverity eventDateAndTime eventSource days

Schwachstelle	Beschreibung	Parameter
eventTaskInternalError	Fehler bei Aufgabenausführung	eventSeverity eventDateAndTime eventSource errorCode knowledgeBaseId taskName
eventUpdateError	Fehler bei Ausführung einer Aufgabe zum Update	eventSeverity eventDateAndTime taskName updaterErrorEventReason

Die Schwachstellen-Parameter und mögliche Parameterwerte stehen in der folgenden Tabelle.

Parameter	Beschreibung und mögliche Werte
eventDateAndTime	Uhrzeit für Eintreten eines Ereignisses
eventSeverity	Prioritätsstufe des Ereignisses. Mögliche Werte: • critical (1) – kritisch, • warning (2) – Warnung, • info (3)– informativ
UserName	Benutzername (beispielsweise des Benutzers, der versucht hat, Zugriff auf eine infizierte Datei zu bekommen)
computerName	Computername (beispielsweise des Computers, von dem versucht wurde, Zugriff auf eine infizierte Datei zu bekommen)

Parameter	Beschreibung und mögliche Werte
eventSource	Ereignisquelle: Funktionalkomponente, bei der ein Ereignis aufgetreten ist. Mögliche Werte: • unknown (0) – Funktionalkomponente ist nicht bekannt • quarantine (1) – Quarantäne • backup (2) – Backup • reporting (3) – Berichte • updates (4)– Update • realTimeProtection (5) – Echtzeitschutz • onDemandScanning (6) – Virensuche • product (7) – Ereignis, das nicht mit einzelnen Komponenten, sondern mit dem Anti-Virus als Ganzes zu tun hat • systemAudit (8) – Bericht zum System-Audit • hostBlocker (9) – Zugriffssperre von Computern auf Server
eventReason	Grund für Ereigniseintritt. Mögliche Werte: • reasonUnknown (0) – Grund ist unbekannt • reasonInvalidSettings (1) – nur für Ereignisse des Backups und der Quarantäne; wird angezeigt, wenn der Quarantäne-Ordner und der Backup-Ordner nicht zur Verfügung stehen (ungenügende Zugriffsrechte oder Ordner in Quarantäne-Parameter falsch angegeben, zum Beispiel wurde ein Netzwerkpfad eingegeben). In diesem Fall verwendet Anti-Virus den standardmäßigen Backup-Ordner oder Quarantäne-Ordner.
objectName	Name des Objektes (beispielsweise Name der Datei, in der eine Bedrohung erkannt wurde)
threatName	Name der Bedrohung

Parameter	Beschreibung und mögliche Werte
detectType	Bedrohungsart. Mögliche Werte: undefined (0) – unbestimmt virware – klassische Viren und Netzwerkwürmer trojware – Trojanische Programme malware – diverse schädliche Programme adware – Adware pornware – Programme mit pornografischem Inhalt riskware – potentiell gefährliche Programme Details zu den Bedrohungstypen finden Sie in Pkt. 1.1.2 auf S. 15.
detectCertainty	Gewissheit für Erkennung einer Bedrohung. Mögliche Werte: • Warning (Warnung) - das Objekt wurde mit der heuristischen Analysemethode als verdächtig eingestuft. • Suspicion (verdächtig) - das Objekt wurde als verdächtig eingestuft. Es wurde eine partielle Übereinstimmung von Codebestandteilen des Objektes mit Codebestandteilen von einer bekannten Bedrohung festgestellt. • Sure (infiziert) - das Objekt wurde als infiziert eingestuft. Es wurde eine komplette Übereinstimmung von Codebestandteilen des Objektes mit Codebestandteilen von einer bekannten Bedrohung festgestellt.
days	Tage (beispielsweise Tage bis zum Ablauf der Gültigkeitsdauer für den Lizenzschlüssel)
errorCode	Fehlercode
knowledgeBaseId	Adresse des Artikels in der Wissensdatenbank (beispielsweise Adresse des Artikels, der einen Fehler beschreibt)
taskName	Aufgabename
storageObjectNotAddedEventReason	Grund, aus dem das Objekt nicht in den Backup-Speicher verschoben wurde.

Parameter	Beschreibung und mögliche Werte
updaterErrorEvent-Reason	Grund für Nichtübernahme des Updates. Mögliche Werte: • reasonUnknown(0) – Grund ist unbekannt; • reasonAccessDenied – Zugriff verweigert; • reasonUrlsExhausted – Liste mit Updatequellen ist erschöpft; • reasonInvalidConfig – ungültige Konfigurationsdatei; • reasonInvalidSignature – ungültige Signatur; • reasonCantCreateFolder – Ordner kann nicht angelegt werden; • reasonFileOperError – Dateifehler; • reasonDataCorrupted – Objekt wurde beschädigt; • reasonConnectionReset – Verbindungsabbruch; • reasonTimeOut – Wartezeit auf Verbindung wurde überschritten; • reasonProxyAuthError – Fehler bei Authentifizierung am Proxyserver; • reasonServerAuthError – Fehler bei Authentifizierung am Server; • reasonHostNotFound – Computer wurde nicht gefunden; • reasonServerBusy – Dienst steht nicht zur Verfügung; • reasonConnectionError – Verbindungsfehler; • reasonModuleNotFound – Objekt wurde nicht gefunden; • reasonBlstCheckFailed(16) – Fehler beim Überprüfen in Liste mit eingezogenen Lizenzen. Möglicherweise wurde während des Updatevorgangs Datenbank-Updates veröffentlicht. Wiederholen Sie bitte das Update in einigen Minuten. Beachten Sie die Beschreibung der Gründe und die möglichen Aktionen des Administrators auf der Seite des Technischen Kundendienstes im Abschnitt **Wenn das Programm einen Fehler ausgegeben hat** (http://support.kaspersky.com/de/error).

Parameter	Beschreibung und mögliche Werte
storageObjectNotAddedEventReason	Grund für Nichtverschieben eines Objektes in Backup oder Quarantäne. Mögliche Werte: • reasonUnknown(0) – Grund ist unbekannt; • reasonStorageInternalError – Datenbankfehler; Anti-Virus wiederherstellen; • reasonStorageReadOnly – Datenbank kann nur gelesen werden; Anti-Virus wiederherstellen; • reasonStorageIOError – Ein-/Ausgabefehler: a) Anti-Virus wurde beschädigt, Anti-Virus wiederherstellen; b) der Datenträger, auf dem die Anti-Virus-Dateien gespeichert sind, ist beschädigt; • reasonStorageCorrupted – Ablage ist beschädigt; Anti-Virus wiederherstellen; • reasonStorageFull – Datenbank ist voll; Speicherplatz auf Datenträger freigeben; • reasonStorageOpenError – Datenbankdatei konnte nicht geöffnet werden; Anti-Virus wiederherstellen; • reasonStorageOSFeatureError – Einige Besonderheiten des Betriebssystems entsprechen nicht den Anti-Virus-Vorgaben; • reasonObjectNotFound – Das in die Ablage zu verschiebende Objekt fehlt auf dem Datenträger; • reasonObjectAccessError – Rechte für Verwendung der Backup-API reichen nicht: Das Benutzerkonto, mit dessen Rechten der Vorgang ausgeführt wird, hat nicht die Berechtigung Backup Operator. • reasonDiskOutOfSpace – Speicherplatz auf Datenträger reicht nicht aus.

ANHANG A. ANFRAGE AN DEN TECHNISCHEN KUNDENDIENST

Wenn Sie für ein Problem in diesem Handbuch oder in der Wissensdatenbank von Kaspersky Lab (http://support.kaspersky.com/de/) keine Lösung gefunden haben, wenden Sie sich an den Technischen Kundendienst von Kaspersky Lab.

> **Anmerkung**
>
> Um die Leistungen des Technischen Kundendienstes in Anspruch nehmen zu können, teilen Sie dem Mitarbeiter des Technischen Kundendienstes die Nummer Ihrer Lizenzschlüssel-Datei (steht im Dateinamen), die Auftragsnummer und/oder die Kundennummer mit. Um eine Kundennummer zu erhalten, müssen Sie sich auf der Internetseite des Technischen Kundendienstes unter https://support.kaspersky.com/de/PersonalCabinet/Registration/Form/ registrieren und die Seriennummer des Lizenzschlüssels angeben. Außerdem verwenden Sie die Kundennummer für den Zugang zu Ihrem Persönlichen Bereich (https://support.kaspersky.com/de/PersonalCabinet).

Sie können sich auf die folgende Weise mit den Mitarbeitern des Technischen Kundendienstes in Verbindung setzen:

- Dringende Anfragen können Sie an die Telefonnummern richten, die im Abschnitt **Kontaktadressen** (s. Pkt. C.2 auf S. 451) genannt sind. Der Online-Support für Benutzer ist rund um die Uhr besetzt und beantwortet Fragen in Russisch und Englisch. Um einen Spezialisten für die Anwendung Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition zu erreichen, ist es allerdings besser, an Werktagen zwischen 10 und 18 Uhr Moskauer Zeit (GMT +3) anzurufen.

- Sie können den Spezialisten des Technischen Support-Services Ihre Frage stellen. Füllen Sie dazu das Web-Formular im System Helpdesk aus, das sich auf der Seite http://support.kaspersky.ru/helpdesk.html?LANG=de. Die Spezialisten des Technischen Support-Services werden Ihre Fragen über das Personal Cabinet oder per E-Mail an die in der Anfrage angegebene Adresse beantworten.

  Beschreiben Sie bei einer Anfrage über das Web-Formular das aufgetretene Problem möglichst genau. Geben Sie in den obligatorisch auszufüllenden Feldern an:

- **Typ der Anfrage**. Die Fragen, die häufig von Benutzern gestellt werden, sind in einer Liste vorgegeben. Dazu zählen beispielsweise: <Problem bei der Installation/Deinstallation des Produkts> oder <Problem bei der Suche/Desinfektion von Viren>. Wenn Sie kein passendes Thema finden, wählen Sie <Allgemeine Frage>.
- **Name des Produkts**: Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition.
- **Anfragetext**. Beschreiben Sie das Problem möglichst genau.
- **Kundennummer und Kennwort**. Geben Sie die Kundennummer und das Kennwort ein, die sich bei der Anmeldung erhalten haben.
- **E-Mail-Adresse**. An diese Adresse werden die Spezialisten des Technischen Support-Services auf Ihre Frage antworten.

Hinweis

Wenn Sie in Ihrem Personal Cabinet eine Frage stellen, ist es ausreichend, das aufgetretene Problem zu beschreiben. Die Angabe von Kundennummer, Kennwort und E-Mail-Adresse ist nicht erforderlich.

ANHANG B. BESCHREIBUNG DER ALLGEMEINEN PARAMETER DES ANTI-VIRUS; PARAMETER SEINER FUNKTIONEN UND AUFGABEN

B.1. Allgemeine Parameter des Anti-Virus

Sie können die folgenden Parameter des Anti-Virus einstellen:

- Maximale Anzahl der Arbeitsprozesse (s. Pkt. B.1.1 auf S. 376)
- Anzahl der Prozesse für Echtzeitschutz (s. B.1.2 auf S. 377)
- Anzahl der Prozesse für Hintergrundaufgaben zur Virensuche (s. Pkt. B.1.3 auf S. 378)
- Wiederherstellung von Aufgaben (s. Pkt. B.1.4 auf S. 379)
- Aufbewahrungsperiode für Informationen, die im Knoten **Berichte** (s. Pkt. B.1.5 auf S. 380)
- Aufbewahrungsperiode für Informationen, die im Knoten **Bericht zum System-Audit** (s. Pkt. B.1.6 auf S. 380)
- Aktionen beim Wechseln in den Betrieb mit einer unterbrechungsfreien Stromversorgung (s. Pkt. B.1.7 auf S. 381)
- Grenzwerte für Registrierung von Ereignissen (s. Pkt. B.1.8 auf S. 382)
- Erstellung des Protokolls der Ablaufverfolgung (s. Pkt. B.1.9 auf S. 382)
- Erstellung von Speicherauszugsdateien der Anti-Virus-Prozesse (s. Pkt. B.1.10 auf S. 388)

B.1.1. Maximale Anzahl der aktiven Prozesse

<table>
<tr><td>Parameter</td><td>Maximale Anzahl der Prozesse</td></tr>
<tr><td>Beschreibung</td><td>Dieser Parameter bezieht sich auf die Parametergruppe Skalierbarkeit des Anti-Virus. Er aktiviert die maximale Anzahl der Prozesse, die Anti-Virus gleichzeitig starten kann.

In den Arbeitsprozessen werden Aufgaben des Echtzeitschutzes, Scans auf Befehl und Updates ausgeführt.

Eine Steigerung der Anzahl von laufenden Prozessen erhöht die Geschwindigkeit bei der Überprüfung der Dateien und Stabilität des Anti-Virus. Allerdings kann ein erhöhter Wert dieses Parameters kann die Serverproduktivität beinträchtigen und den Bedarf an Arbeitsspeicher erhöhen.

Anmerkung

Bitte beachten Sie, dass in der Administrationskonsole von Kaspersky Administration Kit die Parameter Maximale Anzahl aktiver Prozesse nur für Anti-Virus auf einzelnen Server (im Dialogfenster Einstellungen von Anwendung) eingestellt werden können. Sie können diesen Parameter nicht in den Richtlinieneigenschaften ändern.</td></tr>
<tr><td>Mögliche Werte</td><td>1– 8</td></tr>
<tr><td>Standardwert</td><td>Anti-Virus führt die Skalierung in Abhängigkeit von der Anzahl der Prozessoren auf dem Server automatisch aus:
<table>
<tr><th>Anzahl der Prozessoren</th><th>Maximale Anzahl der aktiven Prozesse</th></tr>
<tr><td>=1</td><td>1</td></tr>
<tr><td>1< Anzahl der Prozesse < 4</td><td>2</td></tr>
<tr><td>≥ 4</td><td>4</td></tr>
</table>
</td></tr>
</table>

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 3.2 auf S. 43
- in der Anwendung Kaspersky Administration Kit, auf S. 20.2 auf S. 302

B.1.2. Anzahl der Prozesse für den Echtzeitschutz

<table>
<tr><td>Parameter</td><td>Anzahl der Prozesse für Echtzeitschutz für Dateien</td></tr>
<tr><td>Beschreibung</td><td>Dieser Parameter bezieht sich auf die Parametergruppe Skalierbarkeit des Anti-Virus.

Mit diesem Parameter können Sie eine feste Anzahl von Prozessen festlegen, in denen Anti-Virus die Aufgaben des Echtzeitschutzes ausführt.

Ein höherer Wert dieses Parameters wird eine Erhöhung der Überprüfungsgeschwindigkeit in den Aufgaben des Echtzeitschutzes für Dateien bewirken. Jedoch, um je mehr Prozesse Anti-Virus benutzt, umso größer wird seine Wirkung auf die gesamte Leistungsfähigkeit des geschützten Servers und Speicherauslastung sein.

Anmerkung

Bitte beachten Sie, dass in der Administrationskonsole von Kaspersky Administration Kit die Parameter Maximale Anzahl aktiver Prozesse nur für Anti-Virus auf einzelnen Server (im Dialogfenster Einstellungen von Anwendung) eingestellt werden können. Sie können diesen Parameter nicht in den Richtlinieneigenschaften ändern.</td></tr>
<tr><td>Mögliche Werte</td><td>Mögliche Werte: 1-N, wobei N ein Wert ist, der vom Parameter Maximale Anzahl aktiver Prozesse angegeben wurde.

Wen Sie für Anzahl der Prozesse für den Echtzeitschutz und Maximale Anzahl aktiver Prozesse den gleichen Wert festlegen, senken Sie den Einfluss von Anti-Virus auf die Geschwindigkeit der Dateiübertragung zwischen Computern und Server, während die Geschwindigkeit des Echtzeitschutzes weiter erhöht wird. Aufgaben zum Update und Aufgaben zur Virensuche mit der Basispriorität Mittel (Normal) werden trotzdem in bereits gestarteten aktiven Anti-Virus-Prozessen ausgeführt, wobei sich die Ausführung von Aufgaben zur Virensuche verlangsamt. Falls die Ausführung einer Aufgabe zum Absturz eines Prozesses führt, ist für seinen Neustart mehr Zeit erforderlich.

Aufgaben zur Virensuche mit der Basispriorität Niedrig (Low) werden immer in einem separaten Prozess oder Prozessen ausgeführt (s. Pkt. B.1.3 auf S. 378).</td></tr>
</table>

<table>
<tr>
<td>Standardwert</td>
<td>Anti-Virus führt die Skalierung in Abhängigkeit von der Anzahl der Prozessoren auf dem Server automatisch aus:
<table>
<tr><th>Anzahl der Prozessoren</th><th>Anzahl der Prozesse für den Echtzeitschutz</th></tr>
<tr><td>=1</td><td>1</td></tr>
<tr><td>> 1</td><td>2</td></tr>
</table>
</td>
</tr>
</table>

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 3.2 auf S. 43
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 20.2 auf S. 302

B.1.3. Anzahl der Prozesse für Aufgaben zur Virensuche im Hintergrund

<table>
<tr>
<td>Parameter</td>
<td>Anzahl der Prozesse für Aufgaben zur Virensuche im Hintergrund</td>
</tr>
<tr>
<td>Beschreibung</td>
<td>Dieser Parameter bezieht sich auf die Parametergruppe Parameter für Skalierbarkeit des Anti-Virus.

Mit Hilfe dieses Parameters können Sie die maximale Anzahl der Prozesse festlegen, in denen Anti-Virus die Aufgaben zur Virensuche im Hintergrundmodus ausführen soll.

Die Anzahl der Prozesse, die Sie durch diesen Parameter festlegen, zählt nicht zur Gesamtzahl der aktiven Prozesse von Anti-Virus, die durch den Parameter Maximale Anzahl aktiver Prozesse bestimmt wird.

Wenn Sie beispielsweise folgende Werte festlegen:
• maximale Anzahl der aktiven Prozesse – 3
• Anzahl der Prozesse für Echtzeitschutz-Aufgaben – 3
• Anzahl der Prozesse für Aufgaben zur Virensuche im Hintergrundmodus – 1

und anschließend die Echtzeitschutz-Aufgabe und eine Aufgabe zur Virensuche im Hintergrundmodus starten, besitzt die Gesamtzahl der aktiven Prozesse kavfswp.exe von Anti-Virus den Wert 4.

In einem aktiven Prozess mit niedriger Priorität können mehrere Aufgaben zur Virensuche ausgeführt werden.</td>
</tr>
</table>

	Sie können die Anzahl der aktiven Prozesse beispielsweise erhöhen, wenn Sie gleichzeitig mehrere Aufgaben im Hintergrundmodus starten, damit jede Aufgabe einen einzelnen Prozess erhält. Die Zuweisung separater Aufgabenprozesse erhöht die Zuverlässigkeit und Geschwindigkeit der Aufgaben.
Mögliche Werte	1-4
Standardwert	1

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 3.2 auf S. 43
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 20.2 auf S. 302

B.1.4. Wiederherstellung von Aufgaben

Parameter	Wiederherstellung von Aufgaben (**Wiederherstellen von Aufgaben ausführen maximal**)
Beschreibung	Dieser Parameter bezieht sich auf die Parametergruppe **Zuverlässigkeitsparameter** des Anti-Virus. Er umfasst die Wiederherstellung von Aufgaben, die mit einem Absturz abgeschlossen wurden, und legt die Anzahl der Wiederherstellungsversuche für Aufgaben zur Virensuche fest. Wenn eine Aufgabe abstürzt, versucht der Anti-Virus-Prozess kavfs.exe, den Prozess, in dem die Aufgabe zum Zeitpunkt des Absturzes ausgeführt wurde, wiederherzustellen. *Wenn die Aufgabenwiederherstellung deaktiviert ist*, stellt Anti-Virus Aufgaben zum Echtzeitschutz und zur Virensuche nicht wieder her. *Wenn die Aufgabenwiederherstellung aktiviert ist*, versucht Anti-Virus, Aufgaben zum Echtzeitschutz wiederherzustellen, bis sie erfolgreich gestartet werden. Die Wiederherstellung von Aufgaben zur Virensuche wird so oft versucht, wie durch diesen Parameter festgelegt.
Mögliche Werte	Eingeschaltet / Ausgeschaltet Versuche zur Wiederherstellung der Aufgaben zur Virensuche: 1-10

Standardwert	Wiederherstellung von Aufgaben aktiviert. Anzahl der Versuche zur Wiederherstellung der Aufgaben zur Virensuche – 2.

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 3.2 auf S. 43
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 20.2 auf S. 302

B.1.5. Vorhalteperiode für Berichte

Parameter	Vorhalteperiode für Berichte (**Berichte und Ereignisse speichern für maximal**)
Beschreibung	Dieser Parameter bestimmt, wie viele Tage die Berichte über die Aufgabenausführung vorgehalten werden, die in der Anti-Virus-Konsole der MMC in dem Knoten **Berichte** angezeigt werden. Sie können diesen Parameter ausschalten, um die Berichte unbegrenzte Zeit zu speichern. In diesem Fall kann die Berichtsdatei eine erhebliche Größe erreichen.
Mögliche Werte	1–365
Standardwert	In den Detailberichten über die Aufgabenausführung löscht Anti-Virus alle Einträge, die älter als 30 Tage sind. Allgemeine Berichte über die Aufgabenausführung werden nach 30 Tagen nach dem beenden der Aufgabe gelöscht.

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 3.2 auf S. 43
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 20.2 auf S. 302

B.1.6. Vorhaltefrist für Ereignisse im Bericht zum System-Audit

Parameter	Vorhaltefrist für Bericht zum System-Audit (**Ereignisse speichern nicht mehr als**)

Beschreibung	Sie können die Periode für das Speichern von Ereignissen begrenzen, die in der Anti-Virus-Konsole in der MMC im Knoten **Bericht zum System-Audit** angezeigt werden.
Mögliche Werte	1–365
Standardwert	Ereignisse aus dem Bericht zum System-Audit lassen sich nicht löschen.

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 3.2 auf S. 43
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 20.2 auf S. 302

B.1.7. Aktionen bei Umgang mit unterbrechungsfreier Stromversorgung

Parameter	Aktionen bei Umgang mit unterbrechungsfreier Stromversorgung
Beschreibung	Dieser Parameter bestimmt die Aktionen, die Anti-Virus ausführt, wenn der Server zur unterbrechungsfreien Stromversorgung gewechselt ist.
Mögliche Werte	• Starten / Nicht starten der Aufgabe zur Virensuche, die nach Zeitplan gestartet werden müssen. • Ausführen / Beenden alle gestarteten Aufgaben zur Virensuche
Standardwert	Standard ist bei Arbeit des Servers mit unterbrechungsfreier Stromversorgung im Anti-Virus: • Er startet die Aufgaben zur Virensuche nicht, die nach Zeitplan gestartet werden müssen. • Er beendet automatisch alle gestarteten Aufgaben zur Virensuche.

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 3.2 auf S. 43
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 20.2 auf S. 302

B.1.8. Grenzwerte für die Ereignisauslösung

Parameter	Grenzwerte für die Ereignisauslösung
Beschreibung	Sie können Grenzwerte für die Ereignisauslösung folgende Ereignisse einstellen: • *Datenbanken sind veraltet* und *Datenbanken sind stark veraltet*. Ereignis entsteht, wenn die Datenbanken nicht aktualisiert werden innerhalb der vom Parameter vorgegebenen Tage seit dem letztes Update herausgegeben wurde. Sie können eine Benachrichtigung für Administrator einstellen, wenn das Ereignis entsteht. • *Eine vollständige Untersuchung des Computers liegt lange zurück*. Das Ereignis entsteht, wenn innerhalb der vorgegebenen Tage keine Aufgabe ausgeführt wird, die mit dem Häkchen **Ausführung der Aufgabe als vollständige Untersuchung des Computers auffassen** versehen ist. Details über den Status "Aufgabe Vollständige Untersuchung des Computers" finden Sie in Pkt. 21.4 auf S. 346.
Mögliche Werte	Anzahl der Tage von 1 bis 365
Standardwert	*Datenbanken sind veraltet* – 7 Tage *Datenbanken sind stark veraltet* – 14 Tage *Eine vollständige Untersuchung des Computers liegt lange zurück* – 30 Tage.

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 3.2 auf S. 43
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 20.2 auf S. 302

B.1.9. Parameter des Protokoll der Ablaufverfolgung

- Erstellung des Protokolls der Ablaufverfolgung (s. Pkt. B.1.9.1 auf S. 383)

- Ordner mit Dateien des Protokolls der Ablaufverfolgung (s. Pkt. B.1.9.2 auf S. 384)
- Genauigkeitsstufe des Protokolls der Ablaufverfolgung (s. Pkt. B.1.9.3 auf S. 385)
- Größe des Protokolls der Ablaufverfolgung (s. Pkt. B.1.9.4 auf S. 386)
- Ablaufverfolgung nur einiger Subsysteme des Anti-Virus (s. Pkt. B.1.9.5 auf S. 386)

B.1.9.1. Protokoll der Ablaufverfolgung erstellen

Parameter	Protokoll der Ablaufverfolgung erstellen (**Debug-Infos in Datei protokollieren**)
Beschreibung	Der Parameter **Protokoll der Ablaufverfolgung erstellen** bezieht sich auf die Parametergruppe **Crash-Diagnose**. Wenn während der Arbeit des Anti-Virus ein Problem aufgetreten ist (z.B. Anti-Virus oder eine Aufgabe werden nicht korrekt beendet oder nicht gestartet) und Sie wollen eine Diagnose durchführen, dann können Sie ein Protokoll zur Ablaufverfolgung erstellen und die Dateien an den Technischen Kundendienst von Kaspersky Lab schicken. Details darüber, wie Sie sich an den Technischen Kundendienst wenden, finden Sie in Pkt. 1.2.3 auf S. 22. Protokoll der Ablaufverfolgung jedes Prozesses wird in separate Datei gespeichert.
Werte und einige Empfehlungen für Benutzung	Protokoll der Ablaufverfolgung wird erstellt / wird nicht erstellt. Um das Erstellen des Protokolls der Ablaufverfolgung einzuschalten, müssen Sie einen Ordner als Speicherplatz für die Journaldateien wählen. Wenn Sie Anti-Virus auf dem geschützten Server über eine Konsole verwalten, die auf einem anderen Computer installiert ist, dann müssen Sie, damit das Protokoll der Ablaufverfolgung für das Subsystem **gui** aktiviert wird, die Parameter des Protokolls der Ablaufverfolgung in der Microsoft Windows Registrierung von diesem Computer angeben und dann die Anti-Virus-Konsole in der MMC schließen und wieder öffnen. • Wenn auf dem Computer eine 32-bit-Version von Microsoft Windows installiert ist: HKEY_LOCAL_MACHINE\Software\KasperskyLab\KAVFSEE \6.0\Trace\Configuration=sub-system=gui;level=info;sink=folder(<Ordner für

	Dateien des Protokolls der Ablaufverfolgung und Pfadangabe>);roll=50000;layout=basic;logging=on • Wenn auf dem Computer eine 64-bit-Version von Microsoft Windows installiert ist: HKEY_LOCAL_MACHINE\Software\Wow6432Node\KasperskyLab\KAVFSEE\6.0\Trace\Configuration=sub-system=gui;level=info;sink=folder(<Ordner für Dateien des Protokolls der Ablaufverfolgung und Pfadangabe>);roll=50000;layout=basic;logging=on Wenn Sie den Pfad zum Ordner angeben, können Sie die Umgebungsvariablen des Systems verwenden. Dagegen können Sie die benutzerdefinierten Umgebungsvariablen nicht verwenden.
Standardwert	Protokoll der Ablaufverfolgung wird nicht erstellt.

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 3.2 auf S. 43
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 20.2 auf S. 302

B.1.9.2. Ordner mit Dateien des Protokolls der Ablaufverfolgung

Parameter	Ordner mit Dateien des Protokolls der Ablaufverfolgung
Beschreibung	Um das Erstellen des Protokolls der Ablaufverfolgung einzuschalten, müssen Sie einen Ordner als Speicherplatz für die Journaldateien wählen.
Werte und einige Empfehlungen für Benutzung	Geben Sie den Ordner auf dem lokalen Datenträger des geschützten Servers ein. Wenn Sie einen Pfad zu einem nicht vorhandenen Ordner eingeben, wird das Protokoll der Ablaufverfolgung nicht erstellt. Bitte benutzen Sie keine Netzwerkverzeichnisse, welche mit dem Befehl SUBST erstellt wurden, als Speicher platz für Protokoll der Ablaufverfolgung. Wenn Sie Anti-Virus auf dem geschützten Server im Remote-Betrieb über die MMC-Konsole verwalten, die auf dem Remote-Desktop des Administrators installiert ist, müssen Sie zur Gruppe der lokalen Administratoren auf dem geschützten Server gehören, um die dort befindlichen Ordner zu sehen.

	Wenn Sie den Pfad zu den Trace-Log-Dateien angeben, können Sie die Umgebungsvariablen des Systems verwenden. Dagegen können Sie die benutzerdefinierten Umgebungsvariablen nicht verwenden.
Standardwert	Nicht vorgegeben

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 3.2 auf S. 43
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 20.2 auf S. 302

B.1.9.3. Genauigkeitsstufe des Protokolls der Ablaufverfolgung

Parameter	Genauigkeitsstufe des Protokolls der Ablaufverfolgung
Beschreibung	Sie können Genauigkeitsstufe des Protokolls (*Debugging-Informationen*, *Informative Ereignisse*, *Wichtige Ereignisse*, *Fehler* oder *Kritische Ereignisse*) auswählen.
Werte und einige Empfehlungen für Benutzung	Die höchste Genauigkeitsstufe ist *Debugging-Informationen*, dabei werden in das Protokoll alle Ereignisse eingetragen. Die niedrigste Stufe ist *Kritische Ereignisse*, dabei werden nur kritische Ereignisse aufgenommen. Bitte beachten Sie, dass das Protokoll der Ablaufverfolgung viel Platz auf dem Datenträger einnehmen kann.
Standardwert	Wenn sie nach dem Erstellen des Protokolls der Ablaufverfolgung die Protokoll-Parameter nicht geändert haben, überwacht Anti-Virus alle Subsysteme mit der Genauigkeitsstufe *Debugging-Informationen*.

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 3.2 auf S. 43
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 20.2 auf S. 302

B.1.9.4. Größe einer Protokolldatei der Ablaufverfolgung

Parameter	Größe einer Protokolldatei der Ablaufverfolgung
Beschreibung	Sie können die maximale Größe der Protokolldatei ändern.
Werte und einige Empfehlungen für Benutzung	1 – 999 MB Sobald die Protokolldatei den Höchstwert erreicht, beginnt Anti-Virus mit Eintragungen in einer neuen Datei. Die vorherige Datei wird gespeichert.
Standardwert	Wenn sie nach dem Erstellen des Protokolls der Ablaufverfolgung die Protokoll-Parameter nicht geändert haben, beträgt die maximale Größe einer Protokolldatei 50 MB.

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 3.2 auf S. 43
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 20.2 auf S. 302

B.1.9.5. Ablaufverfolgung einzelner Subsysteme des Anti-Virus

Parameter	Ablaufverfolgung nur einiger Subsysteme des Anti-Virus.
Beschreibung	Sie können nicht alle, sondern nur einige Subsysteme des Anti-Virus überwachen.
Werte und einige Empfehlungen für Benutzung	Im Dialogfenster für die Einstellung der Anti-Virus-Parameter klicken Sie in der Parametergruppe **Crash-Diagnose** auf die Schaltfläche **Erweitert** und im Dialogfenster **Erweiterte Einstellungen** geben Sie im Feld **Komponenten zum Debuggen** die Codes der Subsysteme ein, die Sie im Protokoll verfolgen wollen. Die Codes müssen mit Komma getrennt sein. Beim Schreiben der Codes beachten Sie die Groß- und Kleinschreibung. Die Codes und Namen der Anti-Virus-Subsysteme stehen in der Tabelle 29 auf S. 387. Anti-Virus übernimmt die Parameter der Ablaufverfolgung des Subsystems gui (Anti-Virus-Snap-In) nach dem neuen Starten der Anti-Virus-Konsole. Die Parameter der Ablaufverfolgung des

	Subsystems AK_conn (Integrationssubsystem für den Administrationsagenten von Kaspersky Administration Kit) werden nach dem Neustart des Administrationsagenten von Kaspersky Administration Kit angewendet. Die Parameter der Ablaufverfolgung für die übrigen Subsysteme des Anti-Virus treten sofort nach dem Speichern der Parameter in Kraft.
Standardwert	Wenn Sie nach dem Erstellen des Protokolls der Ablaufverfolgung die Protokoll-Parameter nicht geändert haben, überwacht Anti-Virus alle Subsysteme des Anti-Virus.

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 3.2 auf S. 43
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 20.2 auf S. 302

In der folgenden Tabelle ist eine Liste der Bezeichnungen von den Subsystemen des Anti-Virus aufgeführt, die zur Protokolldatei hinzugefügt werden können.

Tabelle 29. Bezeichnungsliste der Subsysteme für das Protokoll der Ablaufverfolgung

Code des Subsystems	Name des Subsystems
*	Alle Subsysteme (Standard)
Gui	Anti-Virusausrüstung in MMC
AK_conn	Integrationssystem für den Administrationsagenten Kaspersky Administration Kit
Bl	Verwaltungsprozess; realisiert Verwaltungsaufgaben des Anti-Virus
Wp	Arbeitsprozess; realisiert Anti-Virusschutz-Aufgaben
Blgate	Fernverwatungsprozess des Anti-Virus
Ods	Subsystem des Scans auf Befehl
Oas	Subsystem des Echtzeitschutzes der Dateien
Qb	Subsystem der Quarantäne und Backups
Scandll	Hilfsmodule Anti-Virus-Überprüfung
Core	Subsystem der Hauptfunktion des Anti-Virus
Avscan	Subsystem Anti-Virus-Bearbeitung

Code des Subsystems	Name des Subsystems
Avserv	Subsystem für Verwaltung des Anti-Virus-Kernes
Prague	Subsystem der Hauptfunktion
Scsrv	Subsystem der Anfragenverwaltung für die Skript-Interception
Script	Skript-Interception
Updater	Subsystem für Update der Datenbanken- und Programm-Module

B.1.10. Speicherauszugsdateien für Anti-Virus-Prozesse erstellen

Parameter	Speicherauszugsdateien für Anti-Virus-Prozesse erstellen (**Bei Crash Dump-Dateien erstellen**)
Beschreibung	Der Parameter **Bei Crash Dump-Dateien erstellen** bezieht sich auf die Parametergruppe **Crash-Diagnose**. Wenn während der Arbeit des Anti-Virus Probleme auftreten (z.B. Anti-Virus wurde nicht korrekt beendet) und Sie wollen eine Diagnose durchführen, um das Problem zu beheben, dann können Sie ein Speicherauszug für Anti-Virusprozesse erstellen und die Dateien an das Technische Support «Kaspersky Lab» schicken. Details darüber, wie Sie sich an den Technischen Kundendienst wenden, finden Sie in Pkt. 1.2.3 auf S. 22.
Werte und einige Empfehlungen für Benutzung	Speicherauszugsdateien werden erstellt / nicht erstellt. Um das Erstellen der Speicherauszugsdateien zu aktivieren, wählen Sie einen Ordner, in dem die Dateien gespeichert werden. **Anmerkung** Wenn Sie einen nicht vorhandenen Ordner angeben, wird das Protokoll der Ablaufverfolgung nicht erstellt. Wenn Sie Anti-Virus auf dem geschützten Server über die Anti-Virus-Konsole in der MMC verwalten, die auf einem anderen Computer installiert ist, dann müssen Sie, damit das Erstellen von Speicherauszügen von der Anti-Virus-Konsole aktiviert wird, die Parameter für die Erstellung von Speicherauszugsdateien in der Microsoft Windows Registrierung von diesem Computer an-

	geben und dann die Anti-Virus-Konsole schließen und wieder öffnen.
	Wenn auf dem Computer eine 32-bit-Version von Microsoft Windows installiert ist:
	`HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\KAVFSEE\6.0\CrashDump\Enable=0x00000000`
	`HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\KAVFSEE\6.0\CrashDump\Folder=C:\Temp`
	Wenn auf dem Computer eine 64-bit-Version von Microsoft Windows installiert ist:
	`HKEY_LOCAL_MACHINE\Software\Wow6432Node\KasperskyLab\KAVFSEE\6.0\CrashDump\Enable=0x00000000`
	`HKEY_LOCAL_MACHINE\Software\Wow6432Node\KasperskyLab\KAVFSEE\6.0\CrashDump\Folder=C:\Temp`
	`0x00000000` – Erstellen der Speicherauszugsdateien von der Anti-Virus-Konsole in der MMC
	`0x00000001` – Erstellen der Speicherauszugsdateien von der Anti-Virus-Konsole in der MMC
	`Folder=C:\Temp` – Ordner, in dem die Speicherauszugsdatei von der Anti-Virus-Konsole in der MMC bei einem Absturz gespeichert wird.
	Wenn Sie den Pfad zum Ordner mit den Speicherauszugsdateien angeben, können Sie die Umgebungsvariablen des Systems verwenden. Dagegen können Sie die benutzerdefinierten Umgebungsvariablen nicht verwenden.

Standardwert	Speicherauszugsdateien werden nicht erstellt.

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 3.2 auf S. 43
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 20.2 auf S. 302

B.2. Parameterbeschreibung für Aufgabenzeitplan

Sie können folgende Parameter des Aufgabenzeitplans einstellen.

- Starthäufigkeit (s. Pkt. B.2.1 auf S. 390)

- Anfangsdatum des Zeitplans und Uhrzeit des ersten Aufgabenstarts (s. Pkt. B.2.2 auf S. 391)
- Enddatum des Zeitplans (s. Pkt. B.2.3 auf S. 392)
- Maximale Dauer der Aufgabenausführung (s. Pkt. B.2.4 auf S. 393)
- Zeitperiode innerhalb eines Tages, wann die Aufgabe angehalten werden muss (s. Pkt. B.2.5 auf S. 393)
- Übersprungene Aufgaben starten (s. Pkt. B.2.6 auf S. 394)
- Startzeit auf Intervall verteilen, Min. (s. Pkt. B.2.7 auf S. 395)

B.2.1. Starthäufigkeit

Parameter	Starthäufigkeit
Beschreibung	Dieser Parameter ist ein Pflichtparameter. Dieser Aufgabe kann mit der Häufigkeit der von Ihnen vorgegebenen Stunden, Tage oder Wochen, an von Ihnen vorgegebenen Wochentagen, nach dem Starten des Programms oder nach Datenbanken-Update oder erhalten der Updates durch den Administrationsserver.
Werte und einige Empfehlungen für Benutzung	Mögliche Werte: • **Stündlich**. Die Aufgabe wird periodisch gestartet, in der von Ihnen vorgegebenen Anzahl von Stunden. • **Täglich**. Die Aufgabe wird periodisch gestartet, in der von Ihnen vorgegebenen Anzahl von Tage. • **Wöchentlich**. Die Aufgabe wird periodisch gestartet, in der von Ihnen vorgegebenen Anzahl von Wochen an den von Ihnen vorgegebenen Tagen. • **Bei Programmstart**. Die Aufgabe wird bei jedem Anti-Virus-Start gestartet. • **Nach dem Datenbank-Updaten** (Diese Variante wird nicht in den Updateaufgaben benutzt). Die Aufgabe wird nach jedem Update der Anti-Virus-Datenbanken gestartet. • **Nach Update-Download durch Administrationsserver** (wird nur in den Aufgaben **Update der Datenbanken**, **Update der Programm-Module** und **Update-Verteilung** benutzt, wird nur in der Administrationskonsole Kaspersky Administration Kit angezeigt, wird nicht in der Anti-Virus-Konsole MMC angezeigt). Die Aufgabe wird jedes Mal gestartet, sobald der Admi-

	nistrationsserver Datenbanken-Updates empfängt.
Standardwert	In den lokalen Systemaufgaben hat der Parameter **Startfrequenz t** die folgenden Werte: • Echtzeitschutz für Dateien – Beim Programmstart; • Skript-Untersuchung – Beim Programmstart • Überprüfung beim Start des Systems -– Beim Programmstart; • Programmvollständigkeit überprüfen – Beim Programmstart; Arbeitsplatz-Überprüfung – Wöchentlich; • Vollständige Untersuchung des Computers – Wöchentlich (am Freitag um 20:00) • Untersuchung von Quarantäne-Objekten – nach Update der Datenbanken • Update der Programm-Datenbanken – jede Stunde • Update der Programm-Module – Wöchentlich (am Freitag um 16:00); • Update-Verteilung – Zeitplan ist ausgeschaltet • Rollback der Programm-Datenbanken – Zeitplan ist nicht vorgesehen In den neu erstellten Benutzeraufgaben des Scans auf Befehl ist der Zeitplan ausgeschaltet.

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 5.7.1 auf S. 59
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 21.3 auf S. 344

B.2.2. Datum des Inkrafttretens für Zeitplan und Uhrzeit für Aufgabenstart

Parameter	Datum des Inkrafttretens für Zeitplan und Uhrzeit für Aufgabenstart
Beschreibung	Die folgenden Parameter sind Pflichtparameter. • **Datum des Inkrafttretens für Zeitplan (Beginnen am)**. Angefangen von dem gewählten Datum wird Anti-Virus die Aufgabe mit der vorgegebenen Häufigkeit starten. • **Anfangen am** (wird benutzt, wenn Sie als Parameter **Start-**

	frequenz Stündlich gewählt haben). Anti-Virus startet die Aufgabe das erste Mal zu der von Ihnen vorgegebenen Zeit. • **Startzeit** (wird benutzt, wenn Sie als Parameter **Startfrequenz Täglich**, **Wöchentlich** gewählt haben). Anti-Virus startet die Aufgabe zur von Ihnen vorgegebenen Zeit mit einer Häufigkeit, die im Parameter **Startfrequenz** vorgegeben ist.
Mögliche Werte	Geben Sie Datum und Uhrzeit an.
Standardwert	In den neu erstellten Benutzeraufgaben des Scans auf Befehl sind diese Parameter ausgeschaltet. In den lokalen Systemaufgaben haben diese Parameter standardmäßig folgende Werte: • Vollständige Untersuchung des Computers – jeden Freitag um 20.00 Uhr, je nach den Zeiteinstellungen auf dem geschützten Server • Update der Programm-Datenbanken – alle drei Stunden Im Zeitplan anderer Systemaufgaben sind diese Parameter standardmäßig ausgeschaltet.

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 5.7.1 auf S. 59
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 21.3 auf S. 344

B.2.3. Gültigkeitsende für Zeitplan

Parameter	Gültigkeitsende für Zeitplan (**Zeitplan deaktivieren ab**)
Beschreibung	Angefangen an dem von Ihnen definierten Datum tritt der Zeitplan außer Kraft: Die Aufgabe wird nicht mehr nach Zeitplan gestartet. Dieser Parameter wird nicht übernommen, wenn als Parameterwert **Starthäufigkeit Beim Programmstart** oder **Nach Update der Datenbanken** ausgewählt wurde.
Mögliche Werte	Geben Sie Datum ein oder wählen Sie im Dialogfenster **Kalender** das Datum.
Standardwert	Nicht vorgegeben

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 5.7.1 auf S. 59
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 21.3 auf S. 344

B.2.4. Maximale Dauer der Aufgabenausführung

Parameter	Maximale Dauer der Aufgabenausführung
Beschreibung	Wenn eine Aufgabe länger dauert, als die von Ihnen vorgegebene Anzahl der Stunden und Minuten, dann wird die Aufgabe vom Anti-Virus gestoppt. Wenn eine Aufgabe so beendet wird, wird sie nicht als übersprungen betrachtet. Mit diesem Parameter können Sie auch die Zeit des automatischen Stopps für die Aufgaben des Echtzeitschutzes vorgeben. Dieser Parameter wird nicht in den Aufgaben zum Update benutzt.
Mögliche Werte	Geben Sie die Anzahl der Stunden und Minuten an.
Standardwert	Ausgeschaltet

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 5.7.1 auf S. 59
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 21.3 auf S. 344

B.2.5. Zeitperiode in Tagen, in der die Aufgabe angehalten wird

Parameter	Zeitperiode in Tagen, in der die Aufgabe angehalten wird (**Anhalten von…bis**)
Beschreibung	Wenn es nötig ist, können Sie eine Aufgabe für eine vordefinierte Periode innerhalb eines Tages anhalten, z.B. Virensuche anhalten, wenn die Auslastung des Servers um diese Uhrzeit zu hoch ist und Sie möchten nicht, dass der Server durch die Ausführen

	der Aufgabe noch mehr ausgelastet wird . Dieser Parameter wird nicht in den Aufgaben zum Update benutzt. Wenn Sie gleichzeitig mit diesem Parameter auch den Parameter **Maximale Dauer der Aufgabenausführung** eingeschaltet haben, beachten Sie, dass von diesem Parameter vorgegebene Zeit zur allgemeinen Zeit der Aufgabenausführung gehört.
Mögliche Werte	Geben Sie die Zeit innerhalb eines Tages an.
Standardwert	Nicht vorgegeben

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 5.7.1 auf S. 59
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 21.3 auf S. 344

B.2.6. Übersprungene Aufgaben starten

Parameter	Übersprungene Aufgaben starten
Beschreibung	Sie können das Starten von übersprungenen Aufgaben einschalten. Wenn eine Aufgabe nicht nach Zeitplan vom Anti-Virus gestartet wird (z.B. war der Computer ausgeschaltet), betrachtet Anti-Virus diese Aufgabe als *übersprungen* und beginnt sie automatisch, sobald der Computer eingeschaltet wird. Dieser Parameter wird nicht übernommen, wenn Sie als Parameter **Startfrequenz Bei Programmstart** oder **Nach dem Datenbank-Update** ausgewählt haben.
Mögliche Werte	Eingeschaltet / Ausgeschaltet
Standardwert	Ausgeschaltet

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 5.7.1 auf S. 59
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 21.3 auf S. 344

B.2.7. Startzeit auf Intervall verteilen, Min.

Parameter	Startzeit auf Intervall verteilen, Min.
Beschreibung	Wenn Sie einen Wert für diesen Parameter angeben, dann wird die Aufgabe beliebig zwischen berechneter Startzeit nach Zeitplan und berechneter Startzeit nach Zeitplan plus diesen Parameter gestartet. Sie können diesen Parameter anwenden, wenn Sie zum Beispiel einen Sammelrechner benutzen, um die Updates auf mehrere Server zu verteilen, sodass die Belastung des Sammelrechners und des Netzwerkes verringert wird. Dieser Parameter wird nicht benutzt, wenn Sie den Startmodus **Bei Programmstart**, **Nach dem Datenbank-Updaten** oder **Nach Update-Download durch Administrationsserver** gewählt haben.
Mögliche Werte	In Minuten angeben
Standardwert	Nicht vorgegeben

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 5.7.1 auf S. 59
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 21.3 auf S. 344

B.3. Parameter für Sicherheit in Aufgabe *Echtzeitschutz für Dateien* und in den Aufgaben zur Virensuche

In der Aufgabe **Echtzeitschutz für Dateien** und in den Aufgaben zur Virensuche werden folgende Parameter für Sicherheit angewendet:

- Schutzmodus für Objekte (nur in der Aufgabe **Echtzeitschutz für Dateien**) (s. Pkt. B.3.1 auf S. 396)
- Zu untersuchende Objekte (s. Pkt. B.3.2 auf S. 397)
- Nur neue und veränderte Objekte untersuchen (s. Pkt. B.3.3 auf S. 399)
- Untersuchung von zusammengesetzten Objekten (s. Pkt. B.3.4 auf S. 400)
- Aktionen für infizierte Objekte (s. Pkt. B.3.5 auf S. 401)
- Aktionen für verdächtige Objekte (s. B.3.6 auf S. 403)
- Aktionen für Objekte je nach Bedrohungstyp (s. Pkt. B.3.7 auf S. 405)
- Objekte ausschließen (s. Pkt. B.3.8 auf S. 407)
- Bedrohungen ausschließen (s. Pkt.B.3.9 auf S. 408)
- Maximale Dauer der Objekt-Untersuchung (s. Pkt. B.3.10 auf S. 409)
- Maximale Größe des zusammengesetzten Objektes (s. Pkt. B.3.11 auf S. 410)
- iChecker anwenden (s. Pkt. B.3.12 auf S. 410)
- iSwift anwenden (s. Pkt. B.3.13 auf S. 411)

B.3.1. Schutzmodus für Objekte

Der Parameter für Sicherheit **Schutzmodus für Objekte** wird nur in der Aufgabe **Echtzeitschutz für Dateien** benutzt.

Parameter	Schutzmodus für Objekte
Beschreibung	Dieser Parameter wird nur in der Aufgabe **Echtzeitschutz für Dateien** benutzt. Er bestimmt, bei welchen Zugriffsarten auf Objekte Anti-Virus sie untersucht. Der Parameter für Sicherheit **Schutzmodus für Objekte** hat einen allgemeinen Wert für kompletten Schutzbereich, welcher in der Aufgabe vorgegeben ist. Sie können keine unterschiedlichen Werte des Parameters für einzelne Knoten einstellen.
Werte und einige Empfehlungen für Benutzung	Wählen Sie einen Schutzmodus je nach Ihren Wünschen an die Server-Sicherheit und abhängig davon, welche Formate die Dateien auf dem Server haben und welche Information diese Dateien enthalten: • **Intelligenter Modus**. Anti-Virus überprüft Objekt beim Öff-

	nen und überprüft noch mal gleich nach dem Abspeichern, wenn Objekt geändert wurde. Wenn ein Prozess mehrmals auf das Objekt zugreift und es ändert, dann untersucht Anti-Virus das Objekt erst dann noch einmal, wenn dieser Prozess es erneut speichert. • **Beim Öffnen und Ändern**. Anti-Virus untersucht ein Objekt beim Öffnen und untersucht es noch einmal beim Speichern, wenn es geändert wurde. • **Beim Öffnen**. Anti-Virus untersucht ein Objekt beim Öffnen zum Lesen und beim Ausführen und Ändern. • **Beim Ausführen**. Anti-Virus untersucht ein Objekt nur beim Öffnen zum Ausführen. Standardmäßig werden Objekte im Schutzmodus **Beim Öffnen und Ändern** untersucht.

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 6.2.3 auf S. 90
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 21.3 auf S. 344

B.3.2. Zu untersuchende Objekte

Der Parameter für Sicherheit **Zu untersuchende Objekte** wird in der Aufgabe **Echtzeitschutz für Dateien** und in den Aufgaben zur Virensuche benutzt.

Parameter	Zu untersuchende Objekte
Beschreibung	Dieser Parameter bestimmt, ob alle Objekte des Schutzbereiches oder nur die Objekte mit bestimmten Formaten oder bestimmten Erweiterungen untersucht werden sollen. Die Virenanalytiker von Kaspersky Lab stellen Format- und Erweiterungslisten zusammen, die Objekte haben können, wenn sie infiziert sind. Diese Liste ist in den Datenbanken des Anti-Virus enthalten. Wenn sie bei Kaspersky Lab aktualisiert werden, erhalten Sie diese Updates zusammen mit dem Update der Datenbanken. Mit dem Parameter **Zu untersuchende Objekte** können Sie Ihre eigene Erweiterungsliste erstellen.
Werte und einige Empfehlungen für	Wählen Sie einen der folgenden Werte aus: • **Alle Objekte**. Anti-Virus untersucht jedes Objekt, unabhängig

Benutzung	von Dateiendung oder Format. • **Objekte nach Format untersuchen**. Vor der Untersuchung eines Objektes bestimmt Anti-Virus dessen Format. Wenn das Format in der Liste der Formate steht, die für infizierte Objekte in Frage kommen, untersucht Anti-Virus dieses Objekt. Wenn das Format des Objektes nicht in der Liste steht (beispielsweise kann eine Textdatei nicht infiziert werden), überspringt Anti-Virus dieses Objekt. • **Objekte nach der Erweiterungsliste untersuchen**. Anti-Virus untersucht nur die Objekte, deren Erweiterung in der Infektionsliste steht und für eine Infektion in Frage kommt. Wenn die Endung des Objektes nicht in der Liste steht, überspringt Anti-Virus dieses Objekt. Wenn Sie den Wert **Objekte nach Erweiterungsliste untersuchen** wählen, ist das Tempo der Untersuchung höher als bei aktiviertem Wert **Objekte nach Format untersuchen**. Dabei steigt die Infektionsgefahr, denn die Dataiendungen und Formate können nicht übereinstimmen. Wenn zum Beispiel ein Objekt die Endung .txt hat, heißt das nicht, dass dieses Objekt ein Textformat hat. Dieses Objekt kann eine ausführende Datei sein und eine Gefahr darstellen. Jedoch überspringt Anti-Virus es, wenn Dateiendung .txt nicht zur Erweiterungsliste gehört, die für infizierte Objekte in Frage kommen. • **Objekte nach folgenden Erweiterungsmasken untersuchen**. Anti-Virus untersucht Objekte mit den Endungen, die in der von Ihnen eingegebenen Liste stehen (standardmäßig ist die Liste leer). Sie können zur Liste neue Endungen und Masken hinzufügen oder vorhandene Einträge löschen. In den Erweiterungsmasken können Sie Symbole benutzen: * und ?. Sie können alle Erweiterungen aus der Erweiterungsmaske hinzufügen, die mit Anti-Virus geliefert werden. Klicken Sie dazu im Dialogfenster Liste bearbeiten auf die Schaltfläche **Grundeinstellung**. **Laufwerksbootsektoren und MBR**. Dieser Parameter wird benutzt, wenn zum Untersuchungsbereich die vordefinierten Bereiche **Festplatten** und **Wechseldatenträger**, der vordefinierte Bereich **Arbeitsplatz** oder dynamisch erstellte Datenträger. Dieser Parameter wird nicht benutzt, wenn zum Untersuchungsbereich nur die Bereiche **Systemspeicher**, **Autostart-Objekte**, **Gemeinsame Ordner** gehören sowie dann, wenn zum Untersuchungsbereich einzelne Dateien oder Ordner gehören. **Alternative NTFS-Ströme**. Anti-Virus untersucht alternative

	Dateiströme und Ordner auf Datenträgern mit dem NTFS-Dateisystem.

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, in der Aufgabe **Echtzeitschutz für Dateien** – s. Pkt. 6.2.2.2 auf S. 82; in der Aufgabe **Virensuche** – s. Pkt. 9.2.2.2 auf S. 135
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 19.3 auf S. 293

B.3.3. Nur neue und veränderte Objekte untersuchen

Der Sicherheitsparameter **Nur neue und veränderte Objekte untersuchen** wird in der Aufgabe **Echtzeitschutz für Dateien** und in Aufgaben zur Virensuche übernommen.

Parameter	**Nur neue und veränderte Objekte untersuchen**
Beschreibung	Wenn die Untersuchung von nur neuen und geänderten Objekten aktiviert ist, untersucht Anti-Virus alle Objekte des angegebenen Schutzbereiches (Untersuchungsbereiches), bis auf die Objekte, die er nach der erstmaligen Untersuchung als virenfrei eingestuft hat und seit dieser Untersuchung nicht geändert worden sind.
Werte und Empfehlungen zu ihrer Verwendung	**Aktivieren** / **Deaktivieren**

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, in der Aufgabe **Echtzeitschutz für Dateien** – s. Pkt. 6.2.2.2 auf S. 82; in der Aufgabe **Virensuche** – s. Pkt. 9.2.2.2 auf S. 135
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 19.3 auf S. 293

B.3.4. Zusammengesetzte Objekte untersuchen

Der Parameter für Sicherheit **Zusammengesetzte Objekte untersuchen** wird in der Aufgabe **Echtzeitschutz für Dateien** und in den Aufgaben zur Virensuche benutzt.

Parameter	Zusammengesetzte Objekte untersuchen
Beschreibung	Die Untersuchung zusammengesetzter Objekte kann viel Zeit beanspruchen. Standardmäßig überprüft Anti-Virus nur kombinierte Objekte solcher Typen, welche am meisten infizierbar sind und eine höhere Gefahr für den Server darstellen. Zusammengesetzte Objekte der übrigen Typen werden nicht untersucht. Dieser Parameter erlaubt, je nach Ihren Wünschen für die Sicherheit Typen von zusammengesetzten Objekten auszuwählen, die Anti-Virus untersuchen soll.
Werte und einige Empfehlungen für Benutzung	Wählen Sie einen oder mehrere Werte aus: • **Archive**. Anti-Virus untersucht gewöhnliche Archive. Bitte beachten Sie, dass Anti-Virus findet Bedrohungen in den meisten Archiven, desinfizieren kann er aber nur ZIP, ARJ, RAR oder CAB; • **SFX-Archive**. Anti-Virus untersucht das Extrahierungsmodul in den selbst entpackenden SFX-Archiven (self-extracting archive). • **Mail-Datenbanken**. Anti-Virus untersucht Dateien von Mail-Datenbanken aus Microsoft Office Outlook und Microsoft Outlook Express. • **Gepackte Objekte**. Anti-Virus untersucht ausführende Dateien, die von Binär-Packer-Programmen verpackt wurden; wie UPX oder ASPack. Zusammengesetzte Objekte dieses Typs enthalten öfter Bedrohungen als andere Typen. • **Dateien in Mailformaten**. Anti-Virus untersucht Dateien in Mailformaten, z.B. Nachrichten von Microsoft Office Outlook oder Microsoft Outlook Express. • **Eingebettete OLE-Objekte**. Anti-Virus untersucht Objekte, die in Dateien von Microsoft Office eingebettet sind. Microsoft Office-Dokumente umfassen häufig ausführbare Objekte, die Bedrohungen enthalten können. Wenn für den gewählten Schutzbereich (Untersuchungsbereich)

	der Sicherheitsparameter **Nur neue und veränderte Objekte untersuchen** deaktiviert wurde, können Sie diesen Parameter für jeden Typ der zusammengesetzten Objekte einzeln aktivieren oder deaktivieren. Wenn die Untersuchung von nur neuen und geänderten Objekten aktiviert ist, untersucht Anti-Virus alle Objekte des angegebenen Schutzbereiches (Untersuchungsbereiches), bis auf die Objekte, die er nach der erstmaligen Untersuchung als virenfrei eingestuft hat und seit dieser Untersuchung nicht geändert worden sind

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, in der Aufgabe **Echtzeitschutz für Dateien** – s. Pkt. 6.2.2.2 auf S. 82; in der Aufgabe **Virensuche** – s. Pkt. 9.2.2.2 auf S. 135
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 19.3 auf S. 293

B.3.5. Aktion für infizierte Objekte

Der Parameter für Sicherheit **Aktionen für infizierte Objekte** wird in der Aufgabe **Echtzeitschutz für Dateien** und in den Aufgaben zur Virensuche benutzt.

B.3.5.1. In Aufgabe *Echtzeitschutz für Dateien*

Parameter	Aktion für infizierte Objekte
Beschreibung	Wenn Anti-Virus ein Objekt als infiziert erkennt, wird der Zugriff auf das Objekt für Anwendungen gesperrt, die auf dieses Objekt zugreifen. Danach führt Anti-Virus eine von Ihnen definierte Aktion aus. Bevor Anti-Virus das Objekt ändert (desinfiziert oder löscht) wird eine Kopie des Objektes im Backup erstellt. Der Backup ist ein Ordner, in dem die Objekte verschlüsselt aufbewahrt werden. Details über das Backup finden Sie im Kapitel 12 auf S. 189. Anti-Virus versucht ein Objekt zu desinfizieren oder zu löschen, wenn er dessen Kopie nicht zuvor in die Quarantäne verschieben kann. Das Objekt wird übersprungen. Sie können den Grund für das Überspringen des Objektes im Detailbericht über die Aufgabenausführung anzeigen.

Parameterwerte und einige Empfehlungen für Benutzung	Wählen Sie einen der folgenden Werte aus: • **Zugriff sperren + desinfizieren**. Anti-Virus versucht das Objekt zu desinfizieren, und wenn es nicht möglich ist, wird das Objekt nicht verändert (Objekt wird nicht für die Anwendung zugängig sein, welche das Objekt angesprochen hat). • **Zugriff sperren + desinfizieren, irreparable Objekte löschen**. Anti-Virus versucht das Objekt zu desinfizieren, und wenn es nicht möglich ist, wird das Objekt gelöscht. • **Zugriff sperren + löschen**. Anti-Virus löscht das infizierte Objekt. • **Zugriff sperren + empfohlene Aktion ausführen**. Anti-Virus führt automatisch die Aktionen für das Objekt aus, je nach den Bedrohungen, die im Objekt gefunden worden sind und je nach Reparaturwürdigkeit des Objekts. Trojanische Programme werden von Anti-Virus beispielsweise sofort gelöscht, weil sie nicht in andere Dateien eindringen und keine anderen Dateien infizieren, und folglich nicht der Desinfektion unterliegen. • **Zugriff sperren**. Anti-Virus versucht nicht, das Objekt zu desinfizieren oder zu löschen. Der Zugang zum Objekt wird gesperrt.

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 6.2.2.2 auf S. 82
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 19.3 auf S. 293

B.3.5.2. In Aufgaben zur Virensuche

Parameter	Aktion für infizierte Objekte
Beschreibung	Wenn Anti-Virus ein Objekt als infiziert erkennt, führt er die von Ihnen definierte Aktion aus. Bevor Anti-Virus das Objekt ändert (desinfiziert oder löscht) wird eine Kopie des Objektes im Backup erstellt. Der Backup ist ein Ordner, in dem die Objekte verschlüsselt aufbewahrt werden. Details über den Backup finden Sie im Kapitel 12 auf S. 189. Anti-Virus versucht ein Objekt zu desinfizieren oder zu löschen, wenn er dessen Kopie nicht zuvor in die Quarantäne

	verschieben kann. Das Objekt wird nicht verändert. Sie können den Grund für das Überspringen des Objektes im Detailbericht über die Aufgabenausführung anzeigen.
Parameterwerte und einige Empfehlungen für Benutzung	Wählen Sie einen der folgenden Werte aus: • **Desinfizieren**. Anti-Virus versucht das Objekt zu desinfizieren, und wenn es nicht möglich ist, das Objekt wird nicht verändert. • **Desinfizieren, irreparable Objekte löschen**. Anti-Virus versucht das Objekt zu desinfizieren, und wenn es nicht möglich ist, wird das Objekt gelöscht. • **Löschen**. Anti-Virus löscht das infizierte Objekt ohne einen Desinfektionsversuch. • **Empfohlene Aktion ausführen**. Anti-Virus automatisch sucht eine Aktion aus und führt sie für das Objekt aus, entsprechend den Daten über Gefährlichkeit und Reparaturwürdigkeit des Objektes. So löscht Anti-Virus Trojaner sofort, weil sie nicht in andere Dateien eindringen und sie nicht infizieren und deshalb nicht desinfiziert werden können. • **Überspringen**. Das Objekt wird nicht verändert, Anti-Virus versucht es nicht zu desinfizieren. Information über infiziertes Objekt wird im Detailbericht über Aufgabenausführung gespeichert.

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 9.2.2.2 auf S. 135
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 19.3 auf S. 293

B.3.6. Aktion für verdächtige Objekte

Der Parameter für Sicherheit **Aktionen für verdächtige Objekte** wird in der Aufgabe **Echtzeitschutz für Dateien** und in den Aufgaben zur Virensuche benutzt.

B.3.6.1. In Aufgabe *Echtzeitschutz für Dateien*

Parameter	Aktionen für verdächtige Objekte
Beschrei-	Wenn Anti-Virus ein Objekt als verdächtig erkennt, wird der Zu-

bung	gang zum Objekt gesperrt, außerdem führt er für das Objekt eine von Ihnen definierte Aktion aus. Bevor Anti-Virus das Objekt löscht, wird eine Kopie des Objektes im Backup erstellt. Das Backup ist ein Verzeichnis, wo die Objekte verschlüsselt aufbewahrt werden. Details über das Backup finden Sie im Kapitel 12 auf S. 189.
Werte und einige Empfehlungen für Benutzung	Wählen Sie einen der folgenden Werte aus: • **Zugriff sperren + in Quarantäne verschieben**. Das Objekt wird in einen speziellen Ordner verschoben (Quarantäne), wo es verschlüsselt aufbewahrt wird. Details über die Quarantäne finden Sie im Kapitel 11 auf S. 170. • **Zugriff sperren + löschen**. Anti-Virus löscht das verdächtige Objekt vom Datenträger. Anti-Virus versucht ein Objekt zu desinfizieren oder zu löschen, wenn er dessen Kopie nicht zuvor in die Quarantäne verschieben kann. Das Objekt wird nicht verändert. Sie können den Grund für das Überspringen des Objektes im Detailbericht über die Aufgabenausführung anzeigen. • **Zugriff sperren + empfohlene Aktion ausführen**. Anti-Virus sucht eine Aktion aus und führt sie für das Objekt aus, entsprechend den Daten über Gefährlichkeit des Objektes. • **Zugriff sperren**. Anti-Virus versucht nicht, das Objekt zu desinfizieren oder zu löschen, der Zugang zum Objekt wird gesperrt.

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 6.2.2.2 auf S. 82
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 19.3 auf S. 293

B.3.6.2. In Aufgaben zur Virensuche

Parameter	Aktionen für verdächtige Objekte
Beschreibung	Wenn Anti-Virus ein Objekt als verdächtig erkennt, führt er für das Objekt eine von Ihnen definierte Aktion aus. Bevor Anti-Virus das Objekt löscht, wird eine Kopie des Objektes im Backup erstellt. Das Backup ist ein Ordner, wo die Objekte verschlüsselt aufbewahrt werden. Details über das Backup finden Sie im Kapitel 12 auf S. 189.

Werte und einige Empfehlungen für Benutzung	Wählen Sie einen der folgenden Werte aus: • **In Quarantäne verschieben**. Das Objekt wird in einen speziellen Ordner verschoben (Quarantäne), wo es verschlüsselt aufbewahrt wird. Details über die Quarantäne finden Sie im Kapitel 11 auf S. 170. • **Löschen**. Anti-Virus löscht das verdächtige Objekt vom Datenträger. Anti-Virus versucht ein Objekt zu desinfizieren oder zu löschen, wenn er dessen Kopie nicht zuvor in die Quarantäne verschieben kann. Das Objekt wird nicht verändert. Sie können den Grund für das Überspringen des Objektes im Detailbericht über die Aufgabenausführung anzeigen. • **Empfohlene Aktion ausführen**. Anti-Virus sucht eine Aktion aus und führt sie für das Objekt aus, entsprechend den Daten über Gefährlichkeit des Objektes. • **Überspringen**. Das Objekt wird nicht verändert, Anti-Virus versucht es nicht zu desinfizieren. Information über infiziertes Objekt wird im Detailbericht über Aufgabenausführung gespeichert.

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 9.2.2.2 auf S. 135
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 19.3 auf S. 293

B.3.7. Aktionen je nach Bedrohungstyp

Der Parameter für Sicherheit **Aktionen je nach Bedrohungstyp** wird in der Aufgabe **Echtzeitschutz für Dateien** und in den Aufgaben zur Virensuche benutzt.

Parameter	Aktionen je nach Bedrohungstyp (**Aktionen je nach Bedrohungstyp auswählen**)
Beschreibung	Manche Bedrohungstypen stellen eine größere Gefahr für Server dar als andere. Z.B. kann ein Trojaner wesentlich mehr Schaden anrichten als Adware. Mit dem Parameter dieser Gruppe können Sie verschiedene Anti-Virus-Aktionen für Objekte mit verschiedenen Bedrohungstypen einstellen. Wenn Sie die Werte dieses Parameters aktivieren, übernimmt Anti-Virus diese Parameterwerte anstelle der Parameter **Aktion für infizierte Objekte** und **Aktion für verdächtige Objekte**.

Werte und einige Empfehlungen für Benutzung	Wählen Sie für jeden Bedrohungstyp zwei Aktionen für verdächtige und infizierte Objekte, die Anti-Virus versuchen soll auszuführen, wenn er eine Gefahr des definierten Bedrohungstyps entdeckt. Anti-Virus wird die zweite Aktion für das Objekt ausführen, wenn die erste Aktion nicht ausgeführt werden kann. Anti-Virus übernimmt die vorgegebenen Aktionen für infizierte und verdächtige Objekte gleichermaßen. Wenn Sie beispielsweise als erste Aktion **Desinfizieren** und als zweite Aktion **In Quarantäne verschieben** wählen, verschiebt Anti-Virus ein infiziertes Objekt in die Quarantäne, wenn es nicht desinfiziert werden kann, und verschiebt ein verdächtiges Objekt sofort in die Quarantäne und überspringt die Aktion **Desinfizieren**, wenn verdächtige Objekte nicht desinfiziert werden dürfen. Wenn Sie **Überspringen** als erste Aktion auswählen, steht die zweite Aktion nicht zur Verfügung. Für alle anderen Werte werden zwei Aktionen empfohlen. Bitte beachten Sie, dass in der Liste Bedrohungsklassen *Netzwerkwürmer* und *Klassische Viren* in eine Gruppe *Viren* zusammengestellt sind. Wenn Anti-Virus ein Objekt nicht in den Backup oder in die Quarantäne verschieben kann, führt er nicht die nächstfolgende Aktion für das Objekt aus (zum Beispiel Desinfektion oder Löschen). Das Objekt wird als übersprungen betrachtet. Sie können den Grund für das Überspringen des Objektes im Detailbericht über die Aufgabenausführung anzeigen. In der Liste Bedrohungstypen umfasst der Wert **Unbestimmt** neue Viren, die zurzeit nicht zu den bekannten Typen zählen. Die Bedrohungstypen werden in Pkt. 1.1.2 auf S. 15 näher erläutert.
Standardwert	Ausgeschaltet

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, in der Aufgabe **Echtzeitschutz für Dateien** – s. Pkt. 6.2.2.2 auf S. 82; in der Aufgabe **Virensuche** – s. Pkt. 9.2.2.2 auf S. 135
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 19.3 auf S. 293

B.3.8. Objekte ausschließen

Der Parameter für Sicherheit **Objekte ausschließen** wird in der Aufgabe **Echtzeitschutz für Dateien** und in den Aufgaben zur Virensuche benutzt.

Parameter	Objekte ausschließen
Beschreibung	Mit diesem Parameter können Sie einzelne oder mehrere Dateien nach Dateinamen-Maske von der Untersuchung ausschließen. Wenn Sie große Dateien von der Untersuchung ausschließen, beschleunigen Sie dadurch den Dateiaustausch und die Ausführung der Aufgaben des Scans auf Befehl. Angaben darüber, dass ein Objekt von der Untersuchung ausgeschlossen wurde, werden im Bericht über die Aufgabenausführung registriert (entsprechend den Berichtsparametern, die standardmäßig eingestellt sind). Details zu Berichten finden Sie in Pkt. 13.2 auf S. 204. In den Aufgaben zur Virensuche untersucht Anti-Virus, wenn er einen Prozess im Arbeitsspeicher bearbeitet, die ausführende Datei des Prozesses, selbst wenn diese Datei in der Ausschlussliste steht.
Werte und einige Empfehlungen für Benutzung	Erstellen Sie eine Liste der Dateien. Sie können Dateinamen vollständig oder mit einer Maske angeben. Um die Maske einzugeben, benutzen Sie die Zeichen * und ?.
Standardmäßiger Wert	Liste ist leer

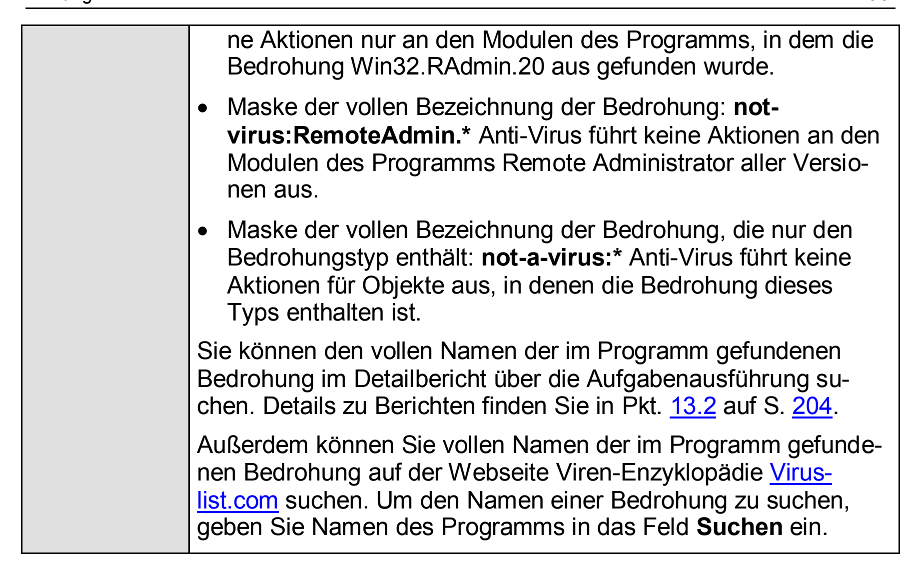
Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, in der Aufgabe **Echtzeitschutz für Dateien** – s. Pkt. 6.2.2.2 auf S. 82; in der Aufgabe **Virensuche** – s. Pkt. 9.2.2.2 auf S. 135
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 19.3 auf S. 293

B.3.9. Bedrohungen ausschließen

Der Parameter für Sicherheit **Bedrohungen ausschließen** wird in der Aufgabe **Echtzeitschutz für Dateien** und in den Aufgaben zur Virensuche benutzt.

Parameter	Bedrohungen ausschließen
Beschreibung	Wenn Anti-Virus ein Objekt als verdächtigen oder infizierten erkennt, und eine Aktion am Objekt eine Aktion unternimmt, Sie jedoch halten dieses Objekt für unbedrohlich für den geschützten Server, dann können Sie die Bedrohung, die vom Anti-Virus im Objekt erkannt wurde, aus der Gefahrenliste des Anti-Virus ausschließen. Sie können eine Bedrohung nach dem Namen in einem konkreten Objekt oder eine ganze Bedrohungsklasse ausschließen. Wenn Sie eine Bedrohung ausschließen, betrachtet Anti-Virus Objekte, die diese Bedrohung enthalten, als virenfrei.
Werte und einige Empfehlungen für Benutzung	Erstellen Sie eine Liste der auszuschließenden Bedrohungen (Liste ist in Grundeinstellung leer). Trennen Sie die Werte in der Liste mit einem Semikolon (;). Um ein Objekt von der Untersuchung auszuschließen, geben Sie den vollen Namen der Bedrohung an, die im Objekt gefunden wurde, also die Ergebniszeile des Anti-Virus, in der steht, dass das Objekt infiziert oder verdächtig ist. Der vollständige Name der Bedrohung wird aufgrund der Objektuntersuchung definiert. Der Name kann die folgenden Information enthalten: **<Bedrohungsklassen>:<Bedrohungstyp>.<Kurzbezeichnung der Plattform>.<Name der Bedrohung>.<Modifikationscode der Bedrohung>**. Zum Beispiel benutzen Sie die Utility Remote Administrator für die Remote-Verwaltung. Viele Antiviren-Anwendungen stufen den Code dieser Utility als Bedrohung vom Typ *Potenziell gefährliches Programm* ein. Damit Anti-Virus das Programm nicht sperrt, fügen Sie den vollständigen Namen der Bedrohung in die Liste der ausgeschlossenen Bedrohungen im Baum der Server-Dateiressourcen ein, in dem die Programmdateien gespeichert sind. Als Parameter können Sie angeben: • Voller Name der Bedrohung: **not-a-virus:RemoteAdmin.Win32.RAdmin.20**. Anti-Virus führt kei-



	ne Aktionen nur an den Modulen des Programms, in dem die Bedrohung Win32.RAdmin.20 aus gefunden wurde. • Maske der vollen Bezeichnung der Bedrohung: **not-virus:RemoteAdmin.*** Anti-Virus führt keine Aktionen an den Modulen des Programms Remote Administrator aller Versionen aus. • Maske der vollen Bezeichnung der Bedrohung, die nur den Bedrohungstyp enthält: **not-a-virus:*** Anti-Virus führt keine Aktionen für Objekte aus, in denen die Bedrohung dieses Typs enthalten ist. Sie können den vollen Namen der im Programm gefundenen Bedrohung im Detailbericht über die Aufgabenausführung suchen. Details zu Berichten finden Sie in Pkt. 13.2 auf S. 204. Außerdem können Sie vollen Namen der im Programm gefundenen Bedrohung auf der Webseite Viren-Enzyklopädie Viruslist.com suchen. Um den Namen einer Bedrohung zu suchen, geben Sie Namen des Programms in das Feld **Suchen** ein.

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, in der Aufgabe **Echtzeitschutz für Dateien** – s. Pkt. 6.2.2.2 auf S. 82; in der Aufgabe **Virensuche** – s. Pkt. 9.2.2.2 auf S. 135
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 19.3 auf S. 293

B.3.10. Maximale Dauer der Objekt-Untersuchung

Der Parameter für Sicherheit **Maximale Dauer der Untersuchung** wird in der Aufgabe **Echtzeitschutz für Dateien** und in den Aufgaben zur Virensuche benutzt.

Parameter	Maximale Dauer der Objektuntersuchung, Sek. (**Untersuchung beenden, wenn sie länger dauert als ... Sek.**)
Beschreibung	Anti-Virus bricht die Untersuchung des Objektes ab, wenn Sie länger dauert als die vorgegebenen Sekunden. Angaben darüber, dass ein Objekt von der Untersuchung ausgeschlossen wurde, werden im Bericht über die Aufgabenausführung registriert (entsprechend den Berichtsparametern, die standardmäßig eingestellt sind).

Werte	Geben Sie die maximale Dauer der Untersuchung in Sekunden an.

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, in der Aufgabe **Echtzeitschutz für Dateien** – s. Pkt. 6.2.2.2 auf S. 82; in der Aufgabe **Virensuche** – s. Pkt. 9.2.2.2 auf S. 135
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 19.3 auf S. 293

B.3.11. Maximale Größe des zu untersuchenden Compound-Objekts

Der Parameter für Sicherheit **Maximale Größe des zu untersuchenden Compound-Objekts** wird in der Aufgabe **Echtzeitschutz für Dateien** und in den Aufgaben zur Virensuche benutzt.

Parameter	Maximale Größe des zu untersuchenden Compound-Objekts, MB (**Komplexe Objekte nicht untersuchen, wenn größer als**)
Beschreibung	Wenn die Größe des zu untersuchenden zusammengesetzten Objektes die vorgegebene Größe übersteigt, überspringt es Anti-Virus. Informationen darüber, dass das Objekt von der Untersuchung ausgeschlossen wurde, wird im Bericht über die Aufgabenausführung registriert (entsprechend den Berichtsparametern, die standardmäßig gelten).
Werte	Geben Sie die maximale Größe des zusammengesetzten Objektes in Megabyte an.

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, in der Aufgabe **Echtzeitschutz für Dateien** – s. Pkt. 6.2.2.2 auf S. 82; in der Aufgabe **Virensuche** – s. Pkt. 9.2.2.2 auf S. 135
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 19.3 auf S. 293

B.3.12. Übernahme von iChecker

Der Parameter für Sicherheit Übernahme von iChecker wird in der Aufgabe **Echtzeitschutz für Dateien** und in den Aufgaben zur Virensuche benutzt.

Parameter	Übernahme von iChecker (**iChecker-Technologie verwenden**)
Beschreibung	Dieser Parameter aktiviert oder deaktiviert iChecker, das von Kaspersky Lab entwickelt worden ist. iChecker wird für Objekte bestimmter Typen und Formate angewendet, die infektionsanfällig sind. iChecker untersucht bereits auf dem Server verarbeitete Objekte nicht noch einmal, die aufgrund von vorangegangenen Untersuchungen von Anti-Virus als nicht infiziert erkannt wurden. Der Einsatz von iChecker senkt die Belastung für den Prozessor und die Datenträger-Systeme und steigert das Tempo der Untersuchung und beschleunigt den Dateiaustausch. Bitte beachten Sie, dass Anti-Virus Objekte nicht wiederholt untersucht, wenn sie seit der letzten Untersuchung geändert wurden, wenn die Parameter für Sicherheit geändert wurden oder weil die Sicherheitsstufe erhöht wurde. Anti-Virus trägt die Information darüber, dass das Objekt aufgrund des Einsatzes von iChecker nicht erneut untersucht worden ist (gemäß den Berichtsparametern, die standardmäßig gelten).
Werte	Eingeschaltet / Ausgeschaltet

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, in der Aufgabe **Echtzeitschutz für Dateien** – s. Pkt. 6.2.2.2 auf S. 82; in der Aufgabe **Virensuche** – s. Pkt. 9.2.2.2 auf S. 135
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 19.3 auf S. 293

B.3.13. Übernahme von iSwift

Der Parameter für Sicherheit Übernahme von iChecker wird in der Aufgabe **Echtzeitschutz für Dateien** und in den Aufgaben zur Virensuche benutzt.

Parameter	Übernahme von iSwift (**iSwift-Technologie verwenden**)
Beschreibung	Dieser Parameter aktiviert oder deaktiviert die von Kaspersky Lab entwickelte Technologie iSwift. Die Technologie iSwift wird für alle Objekte des NTFS-Dateisystems angewendet. iSwift untersucht Objekte nicht noch einmal, die bei vorange-

<table>
<tr><td></td><td>gangenen Untersuchungen von Anti-Virus als nicht infiziert erkannt wurden, sowie Objekte, die andere Antiviren-Programme von Kaspersky Lab in der Version 6.0 untersucht haben. Der Einsatz von iSwift senkt die Belastung für den Prozessor und die Datenträger-Systeme und steigert das Tempo der Untersuchung und beschleunigt den Dateiaustausch.

Bitte beachten Sie, dass Anti-Virus Objekte nicht wiederholt untersucht, wenn sie seit der letzten Untersuchung geändert wurden, wenn die Parameter für Sicherheit geändert wurden oder weil die Sicherheitsstufe erhöht wurde.

Anti-Virus protokolliert Informationen darüber, dass ein Objekt aufgrund der Verwendung von iSwift nicht untersucht wurde (abhängig von den Berichtsparametern, die standardmäßig gelten).

In Anti-Virus wird iNetSwift eingesetzt – die Netzwerkversion von iSwift. Sie funktioniert wie üblich und untersucht Dateien nicht noch einmal. Sie erlaubt die Verarbeitung von Dateien, die von anderen Computern empfangen werden, auf denen eine der folgenden Anwendungen installiert ist und iSwift aktiviert wurde.

• Kaspersky Anti-Virus 6.0 for Windows Workstations
• Kaspersky Anti-Virus 6.0 for Windows Servers
• Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition
• Kaspersky Anti-Virus 6.0 / 7.0
• Kaspersky Internet Security 6.0 / 7.0

Die Verwendung von iNetSwift verhindert die wiederholte Verarbeitung von Objekten innerhalb des gesamten Netzwerks, so dass der Einfluss des Anti-Virus auf das Tempo des Dateiaustausches auf ein Minimum zurückgeführt wird.

Wenn auf dem geschützten Server der Novell Client for Windows XP/2003 Version 4.71 oder höher installiert ist, funktioniert die Technologie iSwift nur innerhalb eines Computers und iNetSwift wird nicht verwendet.</td></tr>
<tr><td>Werte</td><td>Eingeschaltet / Ausgeschaltet</td></tr>
</table>

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, in der Aufgabe **Echtzeitschutz für Dateien** – s. Pkt. 6.2.2.2 auf S. 82; in der Aufgabe **Virensuche** – s. Pkt. 9.2.2.2 auf S. 135
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 19.3 auf S. 293

B.4. Parameter für automatische Zugriffssperre von Computern auf Server

In diesem Anhang werden die folgenden Parameter für die automatische Zugriffssperre von Computern auf den Server beschrieben:

- Einschalten / Ausschalten der automatischen Zugriffssperre von Computern (s. Pkt. B.4.1 auf S. 413)
- Aktionen für infizierte Computer (s. Pkt. B.4.2 auf S. 414)
- Liste der Computer, die von Sperre ausgeschlossen sind (s. Pkt. B.4.3 auf S. 415)
- Funktion Virenepidemien verhindern (s. Pkt. B.4.4 auf S. 416)

B.4.1. Einschalten / Ausschalten der automatischen Zugriffssperre von Computern auf Server

Parameter	Einschalten / Ausschalten der automatischen Zugriffssperre von Computern auf Server
Beschreibung	Dieser Parameter schaltet das automatische Sperren des Zugangs für Computer ein und aus, bei einem Versuch infizierte oder verdächtige Datei auf den Server zu schreiben. Anti-Virus führt keine automatischen Zugriffssperren aus, wenn in der Aufgabe **Echtzeitschutz für Dateien** als Parameterwert **Schutzmodus für Objekte** der Wert **Beim Öffnen** oder **Beim Ausführen** gewählt wurde. In diesem Fall können Sie den Zugang vom infizierten Computer per Hand sperren. Wenn Sie die automatische Zugriffssperre von Computern aktivieren, wird sie nur dann ausgeführt, wenn die Aufgabe **Echtzeitschutz für Dateien** läuft.
Mögliche Werte	Einschalten / Ausschalten

Standardwert	Ausgeschaltet

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 7.2 auf S. 97
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 20.3.1 auf S. 306

B.4.2. Aktionen für infizierte Computer

Parameter	Aktionen für infizierte Computer
Beschreibung	Wenn die automatische Zugriffssperre eingeschaltet ist und ein Computer im lokalen Netzwerk versucht, eine infizierte oder verdächtige Datei auf den Server zu schreiben, führt Anti-Virus die von Ihnen ausgewählten Aktionen aus. Sie können eine oder zwei Aktionen angeben: • **Zugriff von Computern auf Server sperren**. Anti-Virus sperrt den Zugriff von dem Computer auf den Server für die definierte Periode. • **Ausführbare Datei starten**. Anti-Virus startet auf dem Server die angegebene ausführbare Datei. Die Anweisungen in der ausführbaren Datei können die Aktionen bestimmen, die nicht Anti-Virus, sondern eine andere angegebene Anwendung ausführt. Z. B. kann die ausführbare Datei Befehlszeilen enthalten, deren Ausführung einen infizierten Computer zu den Firewall-Einstellungen hinzufügen. Sie können die Daten des infizierten Computer zum Text der ausführenden Datei mit einem speziellen Parameter für die Anti-Virus-Befehlszeile hinzufügen: %COMPUTER_NAME%. Beim Auswählen der ausführenden Datei können Sie die Befehlszeilen-Schlüssel hinzufügen, die von der zu startenden Anwendung unterstützt werden.
Mögliche Werte	Wenn Sie **Zugriff von Computern auf den Server sperren** gewählt haben, dann geben Sie die Zeitspanne an, für die Sie den Zugriff auf den Server von infizierten Computern sperren wollen, in Tagen, Stunden oder Minuten. Wenn Sie **Ausführende Datei starten** gewählt haben, geben Sie den Namen der Datei an und den kompletten Pfad zur Datei an. Außerdem wählen Sie ein Benutzerkonto, mit dessen Berechtigungen die Datei ausgeführt werden soll. Ausführende Datei

	muss auf dem lokalen Laufwerk des geschützten Servers gespeichert sein. Benutzereintrag, mit Rechten welchen die Datei ausgeführt werden soll, muss auf den geschützten Server oder auf dem Domänen-Kontroller registriert sein.
Standardwert	Sperre für 15 Minuten.

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 7.3 auf S. 98
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 20.3.2 auf S. 308

B.4.3. Liste Vertrauenswürdige Computer

Parameter	**Liste Vertrauenswürdige Computer**
Beschreibung	Sie können eine Liste der Computer erstellen, die von automatischen Sperren ausgeschlossen sind, das sind Computer im lokalen Netzwerk, für die Anti-Virus keine Aktionen ausführt, wenn sie versuchen, von diesem Computer ein infiziertes oder verdächtiges Objekt auf den geschützten Server zu schreiben. Wenn Sie ein bereits gesperrtes Computer zur Liste hinzufügen, wird dieser nicht sofort nach dem Speichern der Parameter freigegeben. Der Computer wird nur nach Ablauf der Sperrfrist oder nach der manuellen Freigabe des Computers freigegeben.
Mögliche Werte	Erstellen Sie eine Liste mit Computern, die von der Sperre ausgeschlossen sind, indem Sie für jeden Computer dessen Netzwerknamen, die IP-Adresse oder den IP-Adressbereich eingeben. Es können nur Netzwerk-NetBIOS-Namen von Computern angegeben werden. Die Angabe von DNS-Namen ist nicht zulässig.
Standardwert	Liste ist leer

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 7.4 auf S. 100
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 20.3.3 auf S. 309

B.4.4. Virenepidemien verhindern

Parameter	**Virenepidemien verhindern**
Beschreibung	Wenn die Funktion *Virenepidemien verhindern* eingeschaltet ist, erhöht Anti-Virus die Schutzebene in der ausgeführten Aufgabe **Echtzeitschutz für Dateien**, sobald die Anzahl der für den Server gesperrten Computer den vorgegebenen Wert erreicht. Anti-Virus verwendet die Parameter für Sicherheit zum gesamten Schutzbereich, die in Tabelle 30 aufgelistet sind. Wenn die Wiederherstellung der Sicherheitsstufe eingeschaltet ist, kehrt Anti-Virus, wenn die Anzahl der gesperrten Computer auf den vorgegebenen Wert sinkt, zu den Werten der Parameter für Sicherheit zurück, die in der Aufgabe **Echtzeitschutz für Dateien** definiert sind. Wenn Sie die Werte der Parameter für Sicherheit, die in Tabelle 30 beschrieben sind, in der laufenden Aufgabe **Echtzeitschutz für Dateien** nach dem automatischen Anheben der Sicherheitsstufe und vor deren Wiederherstellung ändern, werden die neuen Parameterwerte nicht sofort übernommen, sondern erst nach Wiederherstellung der Sicherheitsstufe oder wenn Sie Virenepidemien verhindern deaktiviert haben. Informationen über geänderte Parameter für Sicherheit werden im Bericht zum System-Audit registriert. Die Funktion Virenepidemien verhindern wird nicht angewendet, wenn die Werte der Parameter für Sicherheit in der Aufgabe **Echtzeitschutz für Dateien** durch die Richtlinie von Kaspersky Administration Kit bestimmt werden.
Mögliche Werte	Sie können die folgenden Werte aktivieren: • Die Funktion *Virenepidemien verhindern* einschalten / ausschalten; Anzahl der gesperrten Computer angeben, wenn die Anzahl erreicht wird, hebt Anti-Virus die Sicherheitsstufe an • Wiederherstellung der Sicherheitsstufe einschalten / ausschalten, Anzahl der gesperrten Computer angeben, wenn die Anzahl erreicht wird, stellt Anti-Virus die Sicherheitsstufe automatisch wieder her
Standardwert	Ausgeschaltet Wenn Sie die Funktion *Virenepidemien verhindern* einschalten,

	werden standardmäßig die folgenden Werte benutzt: • Sicherheitsstufe erhöhen – 25 Computer • Sicherheitsstufe wiederherstellen – 15 Computer.

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 7.5 auf S. 102
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 20.3.4 auf S. 310

In der folgenden Tabelle stehen die Werte der Parameter für Sicherheit, die in der Aufgabe **Echtzeitschutz für Dateien** benutzt werden, wenn die Anzahl der gesperrten Computer den vorgegebenen Wert erreicht.

Tabelle 30. Werte der Parameter für Sicherheit in der Funktion *Virenepidemien verhindern*

Sicherheitsparameter	**Wert**
Schutzmodus für Objekte (s. Pkt. B.3.1 auf S. 396)	Beim Öffnen und Ändern
Zu untersuchende Objekte (s. Pkt. B.3.2 auf S. 397)	Nach Format
Nur neue und veränderte Objekte untersuchen (s. Pkt. B.3.3 auf S. 399)	Aktiviert
Aktion für infizierte Objekte (s. Pkt. B.3.5 auf S. 401)	Desinfizieren, löschen, wenn Desinfizieren nicht möglich ist
Aktion für verdächtige Objekte (s. Pkt. B.3.6 auf S. 403)	In Quarantäne verschieben

Sicherheitsparameter	Wert
Compound-Objekte untersuchen (s. Pkt. B.3.4 auf S. 400)	Die folgenden Werte der Parameter werden übernommen: • Alle SFX-Archive • Alle gepackte Objekte • Alle eingebettete OLE-Objekte Die folgenden Werte der Parameter wird nicht geändert: • Archive • Mail-Datenbanken • Dateien in Mail-Formaten
Zusätzliche Datenströme von Dateisystem untersuchen (NTFS) (s. Pkt. B.3.2 auf S. 397)	Eingeschaltet
Bootsektoren und MBR untersuchen (s. Pkt. B.3.2 auf S. 397)	Eingeschaltet
Maximale Dauer der Objekt-Untersuchung (s. Pkt. B.3.10 auf S. 409)	60 Sek.
Maximale Größe des zusammengesetzten Objektes (s. Pkt. B.3.11 auf S. 410)	Nicht aktiviert

Die folgenden Werte der Parameter für Sicherheit werden nicht geändert:

- Objekte ausschließen (s. Pkt. B.3.8 auf S. 407)
- Bedrohungen ausschließen (s. Pkt. B.3.9 auf S. 408)
- iSwift verwenden (s. Pkt. B.3.13 auf S. 411)
- iChecker verwenden (s. Pkt. B.3.12 auf S. 410)

B.5. Parameter von Aufgaben zum Update

In den Aufgaben zum Update übernimmt Anti-Virus die folgenden Parameter:

- Allgemeine Parameter, gleich für alle Aufgaben zum Update:
    - Updatequelle (s. Pkt. B.5.1 auf S. 419)
    - Modus eines FTP-Servers für die Verbindung mit dem geschützten Server (s. Pkt. B.5.2 auf S. 421)
    - Wartezeit für Verbindung mit FTP-Server (s. Pkt. B.5.3 auf S. 421)
    - Parameter für Proxy-Server:
        - Ansprechen eines Proxy-Servers für Verbindung mit verschiedenen Updatequellen (s. Pkt. B.5.4.1 auf S. 422)
        - Adresse des Proxy-Servers (s. Pkt. B.5.4.2 auf S. 423)
        - Authentifizierungsmethode beim Zugriff auf den Proxy-Server (s. Pkt. B.5.4.3 auf S. 424)
    - Regionsoptionen für Optimierung des Update-Download (s. Pkt. B.5.5 auf S. 425)
- Parameter der Aufgabe **Update der Programm-Module**:
    - Updates der Programm-Module kopieren und installieren oder nur auf Vorhandensein prüfen (s. Pkt. B.5.6.1 auf S. 426)
    - Daten über Erscheinen von geplanten Updates der Anti-Virus-Module downloaden (s. Pkt. B.5.6.2 auf S. 427)
- Parameter der Aufgabe **Update-Verteilung**:
    - Update-Zusammensetzung (s. Pkt. B.5.7.1 auf S. 428)
    - Ordner zum Speichern von Updates (s. Pkt. B.5.7.2 auf S. 429).

B.5.1. Updatequelle

Parameter	Updatequelle
Beschreibung	Sie können eine Quelle wählen, woher Anti-Virus die Updates der Datenbanken und Programm-Module bezieht, abhängig vom Update-Schema, das in Ihren Unternehmen benutzt wird (beispielhafte Update-Schemata stehen in Pkt. 10.3 auf S. 153).
Mögliche Werte	Als Updatequelle können Sie auswählen: • **Kaspersky-Lab-Updateserver**. Anti-Virus lädt die Updates von einem der Updateserver von Kaspersky Lab, die sich an unterschiedlichen geographischen Punkten befinden. Die Up-

	dates werden mit HTTP- oder FTP-Protokollen heruntergeladen. • **Administrationsserver von Kaspersky Administration Kit**. Sie können diese Updatequelle auswählen, wenn Sie Kaspersky Administration Kit für die zentrale Verwaltung des Antiviren-Schutzes in Ihren Unternehmen benutzen. Anti-Virus kopiert die Updates auf den geschützten Server von einem im lokalen Netzwerk installierten Administrationsserver von Kaspersky Administration Kit. • **Andere HTTP-, FTP-Server oder Netzwerkressourcen**. Anti-Virus kopiert die Updates aus einer von Ihnen gewählten Quelle: Ordner des FTP- oder HTTP-Servers oder von einen Computer im lokalen Netzwerk. Sie können eine oder mehrere benutzerdefinierte Updatequellen angeben. Anti-Virus greift auf jede angegebene Quelle der Reihe nach zu, wenn die vorherige Quelle nicht verfügbar sein sollte. Sie können eine Reihenfolge eingeben, mit der Anti-Virus vorgehen sein, und Sie können einzelne Quelle aktivieren oder deaktivieren. Sie können den Zugriff von Anti-Virus auf die Update-Server von Kaspersky Lab für die Fälle einstellen, wenn alle benutzerdefinierten Quellen nicht verfügbar sind. **Anmerkung** Wenn Sie Pfade eingeben, können Sie Umgebungsvariablen verwenden. Verwenden Sie eine Umgebungsvariable, die für einen Benutzer bestimmt ist, geben Sie das Benutzerkonto dieses Benutzers für den Aufgabenstart ein (s. Pkt. 5.9 auf S. 65). Sie können keine Ordner auf den verbundenen Netzwerklaufwerken als Updatequelle benutzen.
Standardwert	Eine Liste der Kaspersky-Lab-Server finden Sie in der Datei %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0\Update\updcfg.xml.

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 10.5.1 auf S. 159
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 21.2 auf S. 334

B.5.2. Modus eines FTP-Servers für Verbindung zum geschützten Server

Parameter	Modus eines FTP-Servers für Verbindung zum geschützten Server (**Nach Möglichkeit passiven FTP-Modus verwenden**)
Beschreibung	Für die Verbindung mit den Update-Servern über das FTP-Protokoll benutzt Anti-Virus den passiven Modus eines FTP-Servers: Es wird vorausgesetzt, dass eine Firewall im lokalen Netzwerk eingesetzt wird. Wenn der passive Modus eines FTP-Servers nicht funktioniert, wird automatisch in den aktiven Modus gewechselt.
Mögliche Werte	Entscheiden Sie sich für den Modus des FTP-Servers: Aktivieren oder deaktivieren Sie den passiven FTP-Modus.
Standardwert	Nach Möglichkeit passiven FTP-Modus verwenden

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 10.5.1 auf S. 159
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 21.2 auf S. 334

B.5.3. Wartezeit für Verbindung mit Updatequelle

Parameter	Wartezeit für Verbindung (**Timeout**)
Beschreibung	Dieser Parameter gibt die Wartezeit für eine Verbindung mit der Updatequelle vor.
Mögliche Werte	Geben Sie die Wartezeit in Sekunden an.
Standardwert	10 Sek.

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 10.5.1 auf S. 159

- in der Anwendung Kaspersky Administration Kit, s. Pkt. 21.2 auf S. 334

B.5.4. Proxyserver und dessen Parameter

Anti-Virus benutzt die folgenden Parameter für den Zugang an einem Proxy-Server:

- Zugriff auf den Proxy-Server bei Verbindung mit verschiedenen Updatequellen (s. Pkt. B.5.4.1 auf S. 422)
- Parameter des Proxy-Servers (s. Pkt. B.5.4.2 auf S. 423)
- Authentifizierungsmethode bei Zugriff auf Proxy-Server (s. Pkt. B.5.4.3 auf S. 424)

B.5.4.1. Zugriff auf Proxy-Server bei Verbindung mit Updatequellen

Parameter	Zugriff auf Proxy-Server bei Verbindung mit Updatequellen
Beschreibung	Standardmäßig greift Anti-Virus beim Verbinden mit den Update-Servern von Kaspersky Lab auf den Proxy-Server im Netzwerk zu und beim Verbinden mit benutzerdefinierten Updatequellen (bei HTTP- oder FTP-Servern und bei eingegebenen Computern) umgeht Anti-Virus den Proxy-Server: Es wird vorausgesetzt, dass sich diese Quellen im lokalen Netzwerk befinden. Bitte beachten Sie, dass die Dateierweiterungen der Update-Datenbanken zufällig generiert werden. Wenn auf dem Proxyserver Ihres Netzwerks ein Verbot für das Laden von Dateien mit bestimmten Erweiterungen besteht, wird empfohlen, das Laden von Dateien mit beliebigen Erweiterungen von den Kaspersky-Lab-Updateservern zu erlauben. Eine Liste der Kaspersky-Lab-Server finden Sie in der Datei %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0\Update\updcfg.xml.
Mögliche Werte	• Wenn Sie als Updatequelle die Update-Server von Kaspersky Lab angegeben haben, vergewissern Sie sich, dass das Häkchen in **Proxyserver-Parameter für Verbindung zu Kaspersky-Lab-Updateservern verwenden** steht. • Wenn für die Verbindung mit einem benutzerdefinierten FTP- oder HTTP-Server auf einen Proxy-Server zugegriffen werden muss, setzen Sie das Häkchen in **Proxyserver-Parameter für**

	Verbindung zu anderen Servern verwenden. Sollten Sie dieses Kontrollkästchen aktiviert haben, können Sie den Zugriff auf den Proxy-Server für den Zugang zu den übrigen Updatequellen deaktivieren, also die Quellen, für die nicht auf den Proxy-Server zugegriffen werden muss (beispielsweise Computer im lokalen Netzwerk): Setzen Sie das Häkchen in **Für lokale Adressen keinen Proxyserver verwenden**.
Standardwert	Anti-Virus spricht den Proxy-Server an nur beim Verbinden mit HTTP- oder FTP-Servern von Kaspersky Lab.

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 10.5.1 auf S. 159
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 21.2 auf S. 334

B.5.4.2. Parameter des Proxyservers

Parameter	Parameter des Proxyservers
Beschreibung	Bei einer Verbindung mit FTP- oder HTTP-Servern erkennt Anti-Virus automatisch die Parameter des Proxyservers, der im lokalen Netzwerk verwendet wird, und zwar mit dem Web Proxy Auto-Discovery Protocol (WPAD). Sie können manuell die Parameter des Proxyservers eingeben, zum Beispiel für den Fall, wenn das WPAD-Protokoll in Ihrem lokalen Netzwerk nicht eingerichtet ist.
Mögliche Werte	Geben Sie die IP-Adresse oder den DNS-Namen des Servers (zum Beispiel proxy.mycompany.com) und dessen Port ein. Schalten Sie die Benutzung des Proxy-Servers aus, wenn sich der benutzerdefinierte FTP- oder HTTP-Server in Ihrem lokalen Netzwerk befindet.
Standardwert	Parameter des Proxy-Servers automatisch erkennen

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 10.5.1 auf S. 159
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 21.2 auf S. 334

B.5.4.3. Authentifizierungsmethode beim Zugriff auf Proxy-Server

Parameter	Authentifizierungsmethode beim Zugriff auf Proxy-Server
Beschreibung	Dieser Parameter bestimmt die Methode der Authentifizierung eines Benutzers beim Zugriff auf den Proxy-Server, der für die Verbindung mit den FTP- oder HTTP-Servern und den Updatequellen benutzt wird.
Mögliche Werte	Wählen Sie einen der folgenden Werte aus: • **Authentifizierung nicht verwenden**. Wählen Sie diese Variante, wenn für den Zugriff auf den Proxy-Server keine Authentifizierung verlangt wird. • **NTLM- Authentifizierung verwenden**. Anti-Virus benutzt für den Zugriff auf den Proxyserver das Benutzerkonto, unter dem die Aufgabe ausgeführt wird. (Wenn mit dem Aufgabenparameter **Starten als** kein anderes Benutzerkonto vorgegeben ist, wird die Aufgabe unter dem Benutzerkonto **Lokales System (SYSTEM)** ausgeführt. Sie können diese Methode auswählen, wenn der Proxy-Server die in Microsoft Windows integrierte Authentifizierung (NTLM authentication) unterstützt (Näheres zu Benutzerkonten für den Start von Aufgaben finden Sie in Pkt. 5.9.1 auf S. 65). • **NTLM- Authentifizierung mit Name und Kennwort verwenden**. Anti-Virus verwendet das von Ihnen vorgegebene Benutzerkonto für die Authentifizierung am Proxy-Server. Sie können diese Methode wählen, wenn der Proxy-Server die in Microsoft Windows integrierte Authentifizierung unterstützt. Geben Sie das Benutzerkonto und Kennwort ein oder markieren Sie den Benutzer in der Liste. • **Benutzername und Kennwort verwenden**. Sie können die übliche Authentifizierung wählen (Basic authentication). Geben Sie den Benutzernamen und das Kennwort ein oder markieren Sie den Benutzer in der Liste. Sie können diese Methode benutzen, wenn das Benutzerkonto, mit dessen Rechten die Aufgabe zum Update ausgeführt wird, keine Rechte für den Zugang zum Proxy-Server hat und Sie ein anderes Konto benutzen wollen. Wenn die übliche Authentifizierung mit Benutzernamen und Kennwort nicht erfolgreich war, führt Anti-Virus die in Microsoft

	Windows integrierte Authentifizierung aus.
Standardwert	Die Authentifizierung wird beim Zugriff auf den Proxy-Server nicht ausgeführt.

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 10.5.1 auf S. 159
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 21.2 auf S. 334

B.5.5. Regionsoptionen für Optimierung des Update-Downloads (Standort des geschützten Servers)

Parameter	Regionsoptionen für Optimierung des Update-Downloads (**Standort**)
Beschreibung	Die Update-Server von Kaspersky Lab befinden sich an unterschiedlichen geographischen Punkten. Mit diesem Parameter können Sie das Standortland des geschützten Servers angeben. Anti-Virus optimiert den Update-Download von den Kaspersky-Lab-Update-Servern auf den geschützten Server, indem er den in der Nähe stehenden Update-Server ansteuert.
Mögliche Werte	Sie können ein Land für den Standort des geschützten Servers auswählen.
Standardwert	Anti-Virus erkennt standardmäßig den Standort des geschützten Servers je nach dessen Regionsoptionen in Microsoft Windows, für Microsoft Windows Server 2003 nach dem Wert der Variablen **Standort (Location)**, der für das Standardbenutzerprofil (Default User Account Settings) gesetzt ist. Wenn Sie beispielsweise in den Regionsoptionen von Microsoft Windows (unter Ihren aktuellen Benutzerkonto) die Variable **Standort** auf den Wert **Russland** setzen, bleibt für das Standardbenutzerprofil der Wert **USA** erhalten, Anti-Virus greift auf den Update-Server zu, der nicht in Russland, sondern in den Vereinigten Staaten von Amerika steht. Um den Update-Download zu optimieren, nehmen Sie, konnen Sie eine der folgenden Aktionen vor: • in den Regionsoptionen von Microsoft Windows das Land für

	den Standort des Servers durch die Variable **Standort** für das Standardbenutzerprofil angeben; • in Anti-Virus die Update-Aufgabe unter Ihrem aktuellen Benutzerkonto aufrufen; • das Land für den Standort des Servers mit dem Update-Parameter **Standort des geschützten Servers** auswählen, was in dieser Tabelle näher beschrieben ist.

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 10.5.1 auf S. 159
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 21.2 auf S. 334

B.5.6. Parameter der Aufgabe *Update der Programm-Module*

In der Aufgabe **Update der Programm-Module** werden die folgenden Parameter benutzt:

- Updates der kritischen Programm-Module kopieren und installieren oder nur auf Vorhandensein prüfen (s. Pkt. B.5.6.1 auf S. 426)
- Daten über Erscheinen von geplanten Updates der Anti-Virus-Module downloaden (s. Pkt. B.5.6.2 auf S. 427)

B.5.6.1. Kritische Updates der Programm-Module kopieren und installieren oder nur auf Vorhandensein prüfen

Parameter	Kritische Updates der Programm-Module kopieren und installieren oder nur auf Vorhandensein prüfen
Beschreibung	Mit den Parametern der Aufgabe **Update der Programm-Module** können Sie festlegen, ob kritische Updates der Programm-Module gleich geladen und installiert werden sollen oder nur geprüft werden soll, ob Updates vorliegen.
Mögliche Werte	Wählen Sie einen der folgenden Werte aus: • **Nur prüfen, ob kritische Updates für Programm-Module verfügbar sind**. Sie können diese Variante auswählen, um beispielsweise das Erscheinen von dringenden Updates der

	Anti-Virus-Module in Erfahrung zu bringen. • **Verfügbare kritische Updates für Programm-Module kopieren und installieren**.
Standardwert	**Nur prüfen, ob kritische Updates für Programm-Module verfügbar sind**

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 10.5.2 auf S. 164
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 21.2 auf S. 334

B.5.6.2. Daten über Erscheinen von geplanten Updates der Anti-Virus-Module downloaden

Parameter	Daten über Erscheinen von geplanten Updates der Anti-Virus-Module downloaden
Beschreibung	Sie können Daten über das Erscheinen von geplanten Updates der Anti-Virus-Module downloaden. Um Benachrichtigungen über das Erscheinen von geplanten Updates zu laden, aktivieren Sie den Wert **Informationen über verfügbare geplante Updates für Programm-Module empfangen** und konfigurieren Sie die Benachrichtigung über das Anti-Virus-Ereignis "Update der Programm-Module verfügbar", in der die Adresse unserer Internetseite steht, von der Sie die geplanten Updates downloaden können (Details zur Einstellung von Benachrichtigungen finden Sie in Pkt. 15.2 auf S. 237).
Mögliche Werte	Daten über das Erscheinen von geplanten Updates der Anti-Virus-Module downloaden / nicht downloaden
Standardwert	**Informationen über verfügbare geplante Updates für Programm-Module empfangen**

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 10.5.2 auf S. 164
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 21.2 auf S. 334

B.5.7. Parameter der Aufgabe *Update-Verteilung*

In der Aufgabe **Update-Verteilung** benutzt Anti-Virus die folgenden Parameter:

- Zusammensetzung der Updates in der Aufgabe **Update-Verteilung** (s. Pkt B.5.7.1 auf S. 428)
- Ordner zum Speichern der Updates (s. Pkt B.5.7.2 auf S. 429).

B.5.7.1. Zusammensetzung der Updates

Parameter	Zusammensetzung der Updates
Beschrei-bung	Mit diesem Parameter können Sie die Zusammensetzung der zu kopierenden Updates bestimmen. Sie können nur Updates Anti-Virus-Datenbanken, nur dringende Updates seiner Programm-Module oder alle verfügbaren Updates kopieren. Oder Sie können nicht nur die Updates der Datenbanken und Module von Anti-Virus, sondern auch von anderen Kaspersky-Lab-Anwendungen in der Version 6.0 kopieren, um die empfangenen Updates auf andere Rechner im lokalen Netzwerk zu verteilen, auf denen die Antiviren-Anwendungen von Kaspersky Lab in dieser Version installiert sind. Standardmäßig speichert Anti-Virus die Update-Dateien im Ordner %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0\UpdateDistribution\.
Mögliche Werte	Wählen Sie einen der folgenden Werte aus: • Um in den angegebenen Ordner nur Updates der Datenbanken zu laden und zu speichern, markieren Sie **Updates der Programm-Datenbanken kopieren**. • Um in den angegebenen Ordner nur Updates der Programm-Module zu laden und zu speichern, markieren Sie **Kritische Updates der Programm-Module kopieren**. • Um in den angegebenen Ordner auch Updates der Datenbanken und der Programm-Module zu laden und zu speichern, markieren Sie **Updates der Datenbanken und kritische Updates der Programmmodule kopieren**. Um Updates der Datenbanken und Programm-Module nicht nur

	für den Anti-Virus zu empfangen, sondern auch für die übrigen Kaspersky-Lab-Anwendungen in der Version 6.0 und höher, markieren Sie **Updates der Datenbanken und Module für alle Kaspersky-Lab-Anwendungen der Version 6.0 und höher kopieren**.
Standardwert	Anti-Virus kopiert nur die Updates der Anti-Virus-Datenbanken.

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 10.5.3 auf S. 166
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 21.2 auf S. 334

B.5.7.2. Ordner zum Speichern der Updates

Parameter	Ordner zum Speichern der Updates
Beschreibung	Mit diesem Parameter können Sie den Ordner zum Speichern der Update-Dateien angeben.
Mögliche Werte	Geben Sie einen lokalen Ordner oder einen Netzwerkordner an, in den Anti-Virus die kopierten Update-Dateien speichern soll. Um einen Netzwerkordner anzugeben, geben Sie dessen Namen und Pfad im UNC-Format (Universal Naming Convention) ein. Sie dürfen keine Ordner auf verbundenen Netzwerklaufwerken sowie auf Datenträgern angeben, die mit dem Befehl SUBST erstellt worden sind. Wenn Sie die Pfade angeben, können Sie die Umgebungsvariablen verwenden Verwenden Sie eine Umgebungsvariable, die für einen Benutzer bestimmt ist, geben Sie das Benutzerkonto dieses Benutzers für den Aufgabenstart ein (s. Pkt. 5.9 auf S. 65). Wenn Sie Anti-Virus auf dem geschützten Server im Remote-Betrieb über die MMC-Konsole verwalten, die auf dem Remote-Desktop des Administrators installiert ist, müssen Sie zur Gruppe der lokalen Administratoren auf dem geschützten Server gehören, um die dort befindlichen Ordner zu sehen.
Standardwert	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0\Update\Distribution\ Für Anti-Virus kann die Umgebungsvariable %KAVWSEEAPPDATA% zur Angabe des Anti-Virus-Ordners

	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0\ verwendet werden.

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 10.5.3 auf S. 166
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 21.2 auf S. 334

B.6. Parameterbeschreibung für Quarantäne

Die Quarantäne hat die folgenden Parameter:

- Quarantäne-Ordner (s. Pkt. B.6.1 auf S. 430)
- Maximale Größe der Quarantäne (s. Pkt. B.6.2 auf S. 431)
- Schwellenwert für freien Speicherplatz in Quarantäne (s. Pkt. B.6.3 auf S. 432)
- Ordner für Wiederherstellung (s. Pkt. B.6.4 auf S. 432).

B.6.1. Quarantäne-Ordner

Parameter	Quarantäne-Ordner
Beschreibung	Sie können einen Ordner für die Quarantäne eingeben, der vom Quarantäne-Ordner in der Grundeinstellung abweicht.
Mögliche Werte	Geben Sie einen Ordner auf dem lokalen Datenträger des geschützten Servers (Ordnername und Pfad) ein. Anti-Virus beginnt damit, die Objekte in den im Parameter angegebenen Ordner zu verschieben, wenn Sie den neuen Parameterwert speichern. Wenn der angegebene Quarantäne-Ordner nicht vorhanden oder nicht verfügbar ist, wechselt Anti-Virus wieder zum Quarantäne-Ordner der Grundeinstellung. Wenn Sie den Pfad zum Quarantäne-Ordner angeben, können Sie die Umgebungsvariablen des Systems verwenden. Dagegen können Sie die benutzerdefinierten Umgebungsvariablen nicht verwenden. In einer Cluster-Umgebung Geben Sie als Quarantäne-Ordner keine Ordner auf einem Quorum-Datenträger oder auf Cluster-

	Datenträger an.
Standardwert	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0\ Quarantine\ Für Anti-Virus kann die Umgebungsvariable %KAVWSEEAPPDATA%zur Angabe des Anti-Virus-Ordners %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0\ verwendet werden.

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 11.8 auf S. 185
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 20.4.2 auf S. 316

B.6.2. Maximale Größe der Quarantäne

Parameter	Maximale Größe der Quarantäne
Beschreibung	Dieser Parameterwert bestimmt die maximale Größe der Quarantäne – die Gesamtgröße der Daten im Quarantäne-Ordner. Der Parameter **Maximale Größe der Quarantäne** besitzt informativen Charakter. Er begrenzt die Größe der Quarantäne nicht, sondern dient als Kriterium zum Registrieren eines Ereignisses und erlaubt dem Administrator, den Zustand des Speichers zu überwachen. Wenn die maximale Größe der Quarantäne erreicht wurde, speichert Anti-Virus weiterhin verdächtige Objekte darin. Sie können eine Benachrichtigung über das Ereignis einrichten, dass die maximale Größe der Quarantäne überschritten wurde. Anti-Virus verschickt die Benachrichtigung, sobald der gesamte Umfang der Daten den vordefinierten Wert erreicht (s. Kapitel 15 auf S. 235). Empfohlener Wert: 200 MB
Mögliche Werte	1– 999 MB
Standardwert	nicht aktiviert

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 11.8 auf S. 185

- in der Anwendung Kaspersky Administration Kit, s. Pkt. 20.4.2 auf S. 316

B.6.3. Schwellenwert für freien Speicherplatz in Quarantäne

Parameter	Schwellenwert für freien Speicherplatz in Quarantäne
Beschreibung	Dieser Parameter wird zusammen mit dem Parameter **Maximale Größe der Quarantäne** verwendet. Der Parameter **Grenzwert für freien Speicherplatz** besitzt informativen Charakter. Er begrenzt die Größe der Quarantäne nicht, sondern erlaubt es Informationen über deren bevorstehende Überfüllung zu erhalten. Wenn der freie Platz im Quarantäne-Ordner den festgelegten Grenzwert unterschreitet, registriert Anti-Virus das Ereignis **Maximale Größe des Backup-Speichers wurde überschritten** und isoliert verdächtige Objekte weiterhin. Sie können eine Benachrichtigung für das Ereignis **Der Grenzwert für freien Speicherplatz in der Quarantäne wurde überschritten** einrichten (Informationen zum Anpassen von Benachrichtigungen finden Sie in Kapitel 15 auf S. 235).
Mögliche Werte	Geben Sie den Umfang in MB an. Er muss kleiner sein, als der Parameterwert **Maximale Größe des Backups**. Empfohlener Wert: 50 MB
Standardwert	nicht aktiviert

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 11.8 auf S. 185
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 20.4.2 auf S. 316

B.6.4. Ordner für Wiederherstellung

Parameter	Ordner für Wiederherstellung
Beschreibung	Der Wert dieses Parameters bestimmt einen speziellen Ordner

	für wiederhergestellte Objekte auf dem geschützten Server. Beim Wiederherstellen des Objektes können Sie auswählen, wohin das wiederhergestelltes Objekt gespeichert wird: In den ursprünglichen Pfad, in einen speziellen Ordner für wiederhergestellte Objekte auf dem geschützten Server oder in einen anderen ausgewählten Ordner (auf einem Computer, auf dem die Anti-Virus-Konsole installiert ist oder ein Netzwerkordner).
Mögliche Werte	Geben Sie einen Ordner auf dem lokalen Datenträger des geschützten Servers (Ordnername und Pfad) ein. Wenn Sie den Pfad zum Ordner für Wiederherstellung angeben, können Sie die Umgebungsvariablen des Systems verwenden. Dagegen können Sie die benutzerdefinierten Umgebungsvariablen nicht verwenden. Wenn Sie Anti-Virus auf dem geschützten Server im Remote-Betrieb über die MMC-Konsole verwalten, die auf dem Remote-Desktop des Administrators installiert ist, müssen Sie zur Gruppe der lokalen Administratoren auf dem geschützten Server gehören, um die dort befindlichen Ordner zu sehen.
Standardwert	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0\Restored\ Für Anti-Virus kann die Umgebungsvariable %KAVWSEEAPPDATA% zur Angabe des Anti-Virus-Ordners %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0\ verwendet werden.

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 11.8 auf S. 185
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 20.4.2 auf S. 316

B.7. Parameterbeschreibung für Backup

Das Backup hat die folgenden Parameter:

- Backup-Ordner (s. Pkt. B.7.1 auf S. 434)
- Maximale Größe des Backups (s. Pkt. B.7.2 auf S. 435)

- Schwellenwert für freien Speicherplatz im Backup (s. Pkt. B.7.3 auf S. 435)
- Ordner für Wiederherstellung (s. Pkt. B.7.4 auf S. 436).

B.7.1. Backup-Ordner

Parameter	Backup-Ordner
Beschreibung	Sie können einen Ordner für den Backup eingeben, der vom Backup-Ordner in der Grundeinstellung abweicht.
Mögliche Werte	Geben Sie einen Ordner auf dem lokalen Datenträger des geschützten Servers (Ordnername und Pfad) ein. Anti-Virus wechselt sofort zum angegebenen Ordner, sobald Sie die Änderungen übernehmen. Wenn der angegebene Backup-Ordner nicht vorhanden oder nicht verfügbar ist, wechselt Anti-Virus wieder zum Backup-Ordner der Grundeinstellung. Wenn Sie den Pfad zum Backup-Ordner angeben, können Sie die Umgebungsvariablen des Systems verwenden. Dagegen können Sie die benutzerdefinierten Umgebungsvariablen nicht verwenden. In einer Cluster-Umgebung Geben Sie als Backup-Ordner keine Ordner auf einem Quorum-Datenträger oder auf Cluster-Datenträger an. Wenn Sie Anti-Virus auf dem geschützten Server im Remote-Betrieb über die MMC-Konsole verwalten, die auf dem Remote-Desktop des Administrators installiert ist, müssen Sie zur Gruppe der lokalen Administratoren auf dem geschützten Server gehören, um die dort befindlichen Ordner zu sehen.
Standardwert	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0\Backup\ Für Anti-Virus kann die Umgebungsvariable %KAVWSEEAPPDATA% zur Angabe des Anti-Virus-Ordners %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0\ verwendet werden.

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 12.5 auf S. 199

- in der Anwendung Kaspersky Administration Kit, s. Pkt. 20.5.2 auf S. 319

B.7.2. Maximale Größe des Backups

Parameter	Maximale Größe des Backups
Beschreibung	Der Wert dieses Parameters bestimmt die maximale Größe des Backups, also das Datenvolumen im Backup-Ordner. Der Parameter **Maximale Größe des Backups** besitzt informativen Charakter. Er begrenzt die Größe des Backup-Speichers nicht, sondern dient als Kriterium zum Registrieren eines Ereignisses und erlaubt dem Administrator, den Zustand des Speichers zu überwachen. Wenn die maximale Größe des Backup-Speichers erreicht wurde, speichert Anti-Virus weiterhin Kopien infizierter Objekte darin. Sie können eine Benachrichtigung darüber einrichten, dass die maximale Größe des Backups überschritten wurde. Anti-Virus verschickt die Benachrichtigung, sobald der gesamter Umfang der Daten den vordefinierten Wert erreicht (s. Kapitel 15 auf S. 235). Empfohlener Wert: 200 MB
Mögliche Werte	1– 999 MB
Standardwert	nicht aktiviert

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 12.5 auf S. 199
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 20.5.2 auf S. 319

B.7.3. Schwellenwert für freien Speicherplatz im Backup

Parameter	Schwellenwert für freien Speicherplatz im Backup

Beschreibung	Dieser Parameter wird zusammen mit dem Parameter **Maximale Größe des Backups** verwendet. Dieser Parameter besitzt rein informativen Charakter. Er begrenzt die Größe des Backup-Ordners nicht, sondern erlaubt es Informationen über dessen bevorstehende Überfüllung zu erhalten. Wenn der freie Platz im Backup-Ordner den festgelegten Grenzwert unterschreitet, registriert Anti-Virus das Ereignis **Der Grenzwert für freien Speicherplatz im Backup wurde überschritten** und legt weiterhin Kopien infizierter Dateien an. Sie können Benachrichtigungen für Ereignisse dieses Typs einrichten (Informationen zum Anpassen von Benachrichtigungen finden Sie in Kapitel 15 auf S. 235).
Mögliche Werte	Geben Sie den Umfang in MB an. Er muss kleiner sein, als der Parameterwert **Maximale Größe des Backups**. Empfohlener Wert: 50 MB
Standardwert	nicht aktiviert

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 12.5 auf S. 199
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 20.5.2 auf S. 319

B.7.4. Ordner für Wiederherstellung

Parameter	Ordner für Wiederherstellung
Beschreibung	Der Wert dieses Parameters bestimmt einen speziellen Ordner für wiederhergestellte Objekte auf dem lokalen Datenträger des geschützten Servers. Beim Wiederherstellen einer Datei können Sie auswählen, wohin das wiederhergestelltes Objekt gespeichert wird: In den ursprünglichen Pfad, in einen speziellen Ordner für wiederhergestellte Objekte auf dem geschützten Server oder in einen anderen, ausgewählten Ordner (auf einem Computer, wo die Anti-Virus-Konsole installiert ist oder ein Netzwerkordner). Wenn Sie Anti-Virus auf dem geschützten Server im Remote-Betrieb über die MMC-Konsole verwalten, die auf dem Remote-Desktop des Administrators installiert ist, müssen Sie zur Gruppe

	der lokalen Administratoren auf dem geschützten Server gehö-ren, um die dort befindlichen Ordner zu sehen.
Mögliche Werte	Geben Sie einen Ordner auf dem lokalen Datenträger des ge-schützten Servers (Ordnername und Pfad) ein. Wenn Sie den Pfad zum Ordner für Wiederherstellung angeben, können Sie die Umgebungsvariablen des Systems verwenden. Dagegen können Sie die benutzerdefinierten Umgebungsvariab-len nicht verwenden.
Standardwert	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0\Restored\ Für Anti-Virus kann die Umgebungsvariable %KAVWSEEAPPDATA% zur Angabe des Anti-Virus-Ordners %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0\ verwendet werden.

Informationen über die Konfiguration des Parameters:

- in der Anti-Virus-Konsole in der MMC, s. Pkt. 12.5 auf S. 199
- in der Anwendung Kaspersky Administration Kit, s. Pkt. 20.5.2 auf S. 319

ANHANG C. KASPERSKY LAB

Das Unternehmen

Kaspersky Lab ist ein weltweit führendes Unternehmen in den Bereichen Viren-, Spam- und Hacker-Schutz. Unser hoch spezialisiertes Viren-Labor reagiert stets schneller als alle anderen auf neue Bedrohungen, so dass unsere innovativen Programme seit vielen Jahren Heimanwender und Unternehmen jeder Größe zuverlässig schützen.

Bereits 1997 wurde Kaspersky Lab von dem russischen Virenexperten Eugene Kaspersky in Moskau gegründet und hat heute unter anderem Niederlassungen in Deutschland, Frankreich, Großbritannien, Polen, Japan, USA und China.

Einzigartige Erfahrung

Weltweit beschäftigt Kaspersky Lab über 550 hochspezialisierte Mitarbeiter, darunter Mitglieder der Computer Anti-Virus Researchers Organisation (CARO) und des Virus Bulletin Technical Advisory Board. Im Laufe vieler Jahre Forschung und Kampf gegen Computerviren haben wir Wissen und Fähigkeiten erworben, die heute unser wertvollstes Kapital darstellen.

Dank unserer weit reichenden Erfahrung sind wir in der Lage, Entwicklungstrends bei Malware vorherzusehen. Dieser einzigartige Vorteil bildet die Basis der Produkte und Dienstleistungen von Kaspersky Lab, so dass wir anderen immer einen Schritt voraus sind und unseren Kunden stets den besten Schutz bieten können.

Kaspersky Anti-Virus

Nach vielen Jahren innovativer Entwicklungen zählt Kaspersky Lab heute zu den führenden Herstellern von Sicherheits-Software. Der hohe Standard unserer Produkte wird durch zahlreiche Auszeichnungen internationaler Forschungseinrichtungen, unabhängiger Testlabors und renommierter Fachpublikationen bestätigt.

Die Programm-Module unseres bekanntesten Programms, Kaspersky Anti-Virus, gewährleisten einen zuverlässigen Schutz für Workstations, Datei- und Web-Server, Mail-Gateways, Firewalls, Pocket-PCs und Smartphones.

Als erstes Unternehmen entwickelte Kaspersky Lab bedeutende Technologien, die heute selbst bei zahlreichen Antiviren-Programmen anderer Hersteller – wie G-Data, Aladdin und F-Secure – als Programm-Kern einen unverzichtbaren Bestandteil bilden. So vertrauen bereits über 200 Millionen Anwender unseren Innovationen, wie dem heuristischen Analysator zur Entdeckung noch unbekannter Viren, den Micro-Updates für die Antiviren-Datenbanken und dem ersten umfassenden Virenschutz für Unix/Linux-Systeme.

Komplexe Technologien für Ihre Sicherheit

Moderne Viren und Schadprogramme sind komplexe Bedrohungen, so dass die bisher üblichen Schutzpakete für PCs und Netzwerke häufig nicht mehr ausreichen.

Aus diesem Grund entwickelte Kaspersky Lab mit Kaspersky Anti-Hacker eine Personal Firewall und mit Kaspersky Anti-Spam einen besonders effektiven Spam-Filter. Mit den Produkten von Kaspersky Lab können Sie Ihren Computer und Ihr Netzwerk optimal vor allen modernen virtuellen Gefahren schützen.

Service

Kaspersky Lab bietet seinen Kunden eine ganze Palette zusätzlicher Dienstleistungen, die einen maximalen Schutz garantieren: Die Antiviren-Datenbanken werden stündlich aktualisiert, die Anti-Spam-Dateien 12 bis 24 Mal pro Tag. Zudem steht allen Anwendern ein rund-um-die-Uhr-Support zur Verfügung: Telefonisch oder per E-Mail – in deutscher, englischer, russischer und französischer Sprache.

C.1. Andere Produkte von Kaspersky Lab

Kaspersky Lab News Agent

Das Programm News Agent dient der schnellen Zustellung der Nachrichten von Kaspersky Lab, der Benachrichtigung über das "Virus-Wetter" und über neu erschienene Nachrichten. Das Programm liest in vorgegebenen Zeitabständen von den Kaspersky-Lab-Newsservern eine Liste der verfügbaren Nachrichtenkanäle und der darin enthaltenen Informationen.

News Agent verfügt außerdem über folgende Funktionen:

- Visualisierung des Zustands des "Viren-Wetters" im Infobereich der Taskleiste.
- Abonnieren und Abbestellen der Nachrichtenkanäle von Kaspersky Lab.
- Download von Nachrichten für jeden abonnierten Kanal in festgelegten Zeitabständen. Außerdem erfolgt eine Benachrichtigung über ungelesene Nachrichten.
- Anzeige von Nachrichten der abonnierten Kanäle.
- Anzeige einer Liste der Kanäle und ihrer Status.
- Öffnen der Webseite mit dem vollständigen Nachrichtentext im Browser.

News Agent funktioniert unter dem Betriebssystem Microsoft Windows. Er kann als separates Programm benutzt werden oder zu unterschiedlichen integrierten Lösungen von Kaspersky Lab gehören.

Kaspersky® OnLine Scanner

Dieses Programm ist ein kostenloser Dienst, der den Besuchern der Hersteller-Webseite zur Verfügung steht und die effektive Antiviren-Untersuchung des Computers im Online-Modus erlaubt. Kaspersky OnLine Scanner wird direkt im Browser ausgeführt. Dadurch kann der Benutzer schnell eine Antwort auf Fragen erhalten, die mit einer Infektion durch schädliche Programme verbunden sind. Im Rahmen der Untersuchung kann der Benutzer:

- Archive und Mail-Datenbanken von der Untersuchung ausschließen.
- standardmäßige oder erweiterte Datenbanken für die Untersuchung wählen.
- die Untersuchungsergebnisse in den Formaten txt und html in Berichten speichern.

Kaspersky® OnLine Scanner Pro

Dieses Programm stellt einen Abonnementsdienst dar, der den Besuchern der Hersteller-Webseite zur Verfügung steht und die effektive Antiviren-Untersuchung des Computers und die Desinfektion infizierter Dateien im Online-Modus erlaubt. Kaspersky OnLine Scanner Pro wird direkt im Browser ausgeführt. Im Rahmen der Untersuchung kann der Benutzer:

- Archive und Mail-Datenbanken von der Untersuchung ausschließen.
- standardmäßige oder erweiterte Datenbanken für die Untersuchung wählen.
- die Untersuchungsergebnisse in den Formaten txt und html in Berichten speichern.

Kaspersky Anti-Virus® 7.0

Kaspersky Anti-Virus 7.0 dient dem Schutz eines PCs vor schädlichen Programmen. Dabei werden traditionelle Virenschutzmethoden auf optimale Weise mit neuen proaktiven Technologien vereinigt.

Das Programm erlaubt eine komplexe Antiviren-Untersuchung, die folgende Optionen umfasst:

- Antiviren-Untersuchung des Mail-Datenstroms auf Ebene des Datenübertragungsprotokolls (POP3, IMAP und NNTP für eingehende Mails und SMTP für ausgehende Mails) unabhängig vom verwendeten Mailprogramm, sowie Untersuchung und Desinfektion von Mail-Datenbanken.

- Antiviren-Untersuchung des Internet-Datenstroms, der mit HTTP-Protokoll eintrifft, im Echtzeitschutz-Modus.
- Antiviren-Untersuchung beliebiger einzelner Dateien, Ordner und Laufwerke. Außerdem sind vordefinierte Untersuchungsaufgaben für die Virenanalyse von kritischen Bereichen des Betriebssystems und von Objekten, die beim Start des Betriebssystem Microsoft Windows gestartet werden, vorhanden.

Der Proaktive Schutz umfasst:

- *Kontrolle über Veränderungen im Dateisystem*. Das Programm erlaubt es, eine Liste der Anwendungen anzulegen, deren Komponentenbestand kontrolliert werden soll. Dadurch lässt sich die Verletzung der Integrität von Anwendungen durch Schadprogramme verhindern.
- *Überwachung von Prozessen im Arbeitsspeicher*. Kaspersky Anti-Virus 7.0 warnt den Benutzer rechtzeitig, wenn gefährliche, verdächtige oder versteckte Prozesse auftreten oder wenn aktive Prozesse auf unerlaubte Weise verändert werden.
- *Überwachung von Veränderungen in der Registrierung des Betriebssystems* durch die Kontrolle des Zustands der Systemregistrierung.
- Die *Rootkit-Suche* zur Kontrolle von versteckten Prozessen erlaubt es, Bedrohungen abzuwehren, die unter Verwendung der Rootkit-Technologie schädlichen Code im Betriebssystem verstecken.
- *Heuristische Analyse.* Bei der Untersuchung eines Programms emuliert der heuristische Analysator seine Ausführung und protokolliert alle verdächtigen Aktionen wie beispielsweise das Öffnen einer Datei, das Schreiben in eine Datei, das Abfangen von Interrupt-Vektoren usw. Auf der Grundlage dieses Protokolls wird darüber entschieden, ob das Programm eine Vireninfektion verursachen kann. Die Emulation erfolgt isoliert in einer virtuellen Umgebung, wodurch eine Infektion des Computers ausgeschlossen wird.
- *Systemwiederherstellung* nach schädlicher Einwirkung von Spyware: Die Wiederherstellung wird durch die Speicherung aller Veränderungen in der Registrierung und im Dateisystem des Computers und durch das vom Benutzer initiierte Rückgängigmachen der Veränderungen ermöglicht.

Kaspersky® Internet Security 7.0

Kaspersky Internet Security 7.0 ist eine komplexe Lösung für den Schutz eines PCs vor den wichtigsten Bedrohungen (Viren, Hackerangriffe, Spam und Spyware), denen Informationen unterliegen. Alle Komponenten lassen sich über eine einheitliche Benutzeroberfläche einstellen und steuern.

Die Funktion des Antiviren-Schutzes umfasst:

- *Antiviren-Untersuchung des Mail-Datenstroms* auf Ebene des Datenübertragungsprotokolls (POP3, IMAP und NNTP für eingehende Mails und SMTP für ausgehende Mails) unabhängig vom verwendeten Mailprogramm. Für die populären Mailprogramme Microsoft Office Outlook, Microsoft Outlook Express und The Bat! sind Plug-Ins und die Desinfektion von Mail-Datenbanken vorgesehen.

- *Antiviren-Untersuchung des Internet-Datenstroms*, der mit HTTP-Protokoll eintrifft, im Echtzeitschutz-Modus.

- *Schutz des Dateisystems*: Der Antiviren-Untersuchung können beliebige einzelne Dateien, Ordner und Laufwerke unterzogen werden. Außerdem sind vordefinierte Untersuchungsaufgaben für die Virenanalyse von kritischen Bereichen des Betriebssystems und von Objekten, die beim Start des Betriebssystem Microsoft Windows gestartet werden, vorhanden.

- *Proaktiver Schutz*: Das Programm führt die ununterbrochene Überwachung der Aktivität von Anwendungen und Prozessen durch, die im Arbeitsspeicher des Computers gestartet werden, verhindert gefährliche Veränderungen des Dateisystems und der Registrierung, und stellt das System nach schädlicher Einwirkung wieder her.

Der *Schutz vor Internetbetrug* beruht auf dem Erkennen von Phishing-Angriffen. Dadurch lässt sich der Diebstahl Ihrer vertraulichen Informationen verhindern (in erster Linie Kennwörter, Konto- und Kreditkartennummern, sowie Sperren der Ausführung gefährlicher Skripts auf Webseiten, Sperren von Popupfenstern und Werbebannern). Die Funktion zum *Sperren der automatischen Einwahl auf kostenpflichtige Internetressourcen* ermöglicht es, Programme zu identifizieren, die versuchen Ihr Modem für versteckte Verbindungen mit kostenpflichtigen Telefondiensten zu missbrauchen, indem diese Programme gesperrt werden. Das Modul *Schutz von vertraulichen Informationen* gewährleistet den Schutz vor dem unerlaubtem Zugriff und der Übertragung von Informationen mit vertraulichem Charakter. Die Komponente *Kindersicherung* bietet die Kontrolle über den Zugriff von Computerbenutzern auf Internetressourcen.

Kaspersky Internet Security 7.0 *erkennt Versuche zum Scannen der Ports Ihres Computers*, die häufig im Vorfeld von Netzwerkangriffen stattfinden, und wehrt bekannte Netzwerkangriffe erfolgreich ab. Auf der *Basis von vordefinierten Regeln* führt das Programm die Kontrolle aller Netzwerkaktionen durch und überwacht alle *eingehenden und ausgehenden Datenpakete*. Der Stealth-Modus *macht den Computer für die externe Umgebung praktisch unsichtbar*. In diesem Modus wird jede Netzwerkaktivität verboten, wenn sie nicht durch Ausnahmeregeln erlaubt wird, die vom Benutzer festgelegt wurden.

Im Programm wird eine komplexe Methode zur Spam-Filterung eingehender Mails angewandt:

- Untersuchung nach schwarzen und weißen Adressenlisten (einschließlich Adressen von Phishing-Seiten)
- Phrasenuntersuchung im Mailtext
- Analyse des Mailtexts mit Hilfe eines lernfähigen Algorithmus
- Erkennung von Spam in Form von Grafiken

Kaspersky Anti-Virus Mobile

Kaspersky Anti-Virus Mobile bietet den Antiviren-Schutz für mobile Geräte, die mit den Betriebssystemen Symbian OS und Microsoft Windows Mobile arbeiten. Das Programm erlaubt eine komplexe Antiviren-Untersuchung, die folgende Optionen umfasst:

- *Virensuche* des Arbeitsspeichers, der Speicherkarten, einzelner Ordner oder einer konkreten Datei eines mobilen Geräts. Beim Fund eines infizierten Objekts wird es in die Quarantäne verschoben oder gelöscht.
- *Echtzeit-Untersuchung*: Alle eingehenden und veränderten Objekte, sowie Dateien, auf die versucht wird zuzugreifen, werden automatisch untersucht.
- *Schutz vor sms- und mms-Spam*

Kaspersky Anti-Virus für File-Server

Das Produkt schützt die Dateisysteme von Servern, die unter den Betriebssystemen Microsoft Windows, Novell NetWare, Linux und Samba laufen, zuverlässig vor allen Arten schädlicher Programme. Das Produkt umfasst folgende Anwendungen von Kaspersky Lab:

- Kaspersky Administration Kit
- Kaspersky Anti-Virus for Windows Server
- Kaspersky Anti-Virus for Linux File Server
- Kaspersky Anti-Virus for Novell Netware
- Kaspersky Anti-Virus for Samba Server

Vorzüge und Funktionen:

- *Echtzeitschutz der Dateisysteme von Servern*: alle Dateien der Server werden untersucht, wenn versucht wird, sie zu öffnen und auf dem Server zu speichern.
- Verhinderung von Viren-Epidemien
- Virensuche des gesamten Dateisystems oder bestimmter Ordner und Dateien

- Einsatz von Optimierungstechnologien bei der Untersuchung von Objekten des Serverdateisystems
- Systemwiederherstellung nach einer Infektion
- Skalierbarkeit im Rahmen der verfügbaren Systemressourcen
- Berücksichtigung der Systemauslastung
- Verwendung einer Liste mit vertrauenswürdigen Prozessen, deren Aktivität auf dem Server nicht vom Programm kontrolliert wird.
- Remote-Administration des Produkts, einschließlich zentraler Installation, Konfiguration und Steuerung
- Speicherung von Sicherungskopien infizierter und gelöschter Objekte um sie bei Bedarf wiederherzustellen.
- Isolierung verdächtiger Objekte in einem speziellen Speicher
- Benachrichtigungen über Ereignisse bei der Arbeit des Produkts für den Systemadministrator
- Ausführliche Berichtsführung
- Automatisches Update der Datenbanken des Softwareprodukts.

Kaspersky Open Space Security

Kaspersky Open Space Security realisiert eine neue Art des Herangehens an die Sicherheit moderner Unternehmensnetzwerke mit beliebigem Umfang. Dabei gewährleistet es den zentralen Schutz von Informationssystemen und unterstützt externe Arbeitsplätze und mobile Benutzer.

Das Softwareprodukt umfasst vier Produkte:

- Kaspersky Work Space Security
- Kaspersky Business Space Security
- Kaspersky Enterprise Space Security
- Kaspersky Total Space Security

Im Folgenden wird jedes Produkt genau beschrieben.

Kaspersky Work Space Security bietet den zentralen Schutz von Workstations innerhalb und außerhalb eines Unternehmensnetzwerks. Es schützt vor allen aktuellen Internet-Bedrohungen wie Viren, Spyware, Hackerangriffen und Spam.

Vorzüge und Funktionen:

- Komplexer Schutz vor Viren, Spyware, Hackerangriffen und Spam

- Proaktiver Schutz vor neuen Schadprogrammen, die noch nicht in die Datenbanken aufgenommen wurden.
- Personal Firewall mit IDS/IPS-System
- Rollback-Funktion für schädliche Veränderungen im System
- Schutz vor Phishing-Angriffen und Spam
- Dynamisches Ressourcen-Management bei der vollständigen Untersuchung des Systems
- Remote-Administration des Produkts, einschließlich zentraler Installation, Konfiguration und Steuerung
- Unterstützung von Cisco® NAC (Network Admission Control)
- Untersuchung von E-Mails und Internet-Traffic in Echtzeit
- Sperren von Popupfenstern und Werbebannern bei der Arbeit im Internet
- Sichere Arbeit in Netzwerken aller Art, einschließlich Wi-Fi
- Mittel zum Erstellen einer Notfall-CD zur Systemwiederherstellung, um die Folgen von Virenangriffen zu beheben.
- Flexibles Informationssystem für den Schutzstatus
- Automatisches Update der Datenbanken
- Vollständige Unterstützung von 64-Bit-Betriebssystemen
- Optimiert für Notebooks mit Intel® Centrino® Duo
- Möglichkeit zur Remote-Reparatur (Intel® Active Management - Intel® vPro™)

Kaspersky Business Space Security bietet den optimalen Schutz für die Informationsressourcen einer Firma vor Internet-Bedrohungen. Es schützt Workstations und Dateiserver vor Viren, Trojanern und Würmern, und verhindert Virus-Epidemien. Zudem überwacht es die Integrität der Daten und ermöglicht den Benutzern den schnellen Zugriff auf Netzwerkressourcen.

Vorzüge und Funktionen:

- *Remote-Administration* des Produkts, einschließlich zentraler Installation, Konfiguration und Steuerung
- *Unterstützung von Cisco® NAC* (Network Admission Control);
- *Schutz von Workstations und Dateiservern vor allen Internet-Bedrohungen*

- *Verwendung der iSwift-Technologie zur Vermeidung wiederholter Untersuchungen* innerhalb eines Netzwerks
- *Dynamische Auslastung der Serverprozessoren*
- *Isolierung verdächtiger Objekte in einem speziellen Speicher*
- *Rollback-Funktion für schädliche Veränderungen im System*
- *Skalierbarkeit im Rahmen der verfügbaren Systemressourcen*
- *Proaktiver Schutz* für Workstations vor neuen Schadprogrammen, die noch nicht in die Datenbanken aufgenommen wurden.
- *Untersuchung von E-Mail und Internet-Traffic in Echtzeit*
- *Personal Firewall* mit IDS/IPS-System
- *Schutz bei der Arbeit in Wi-Fi-Netzwerken*
- *Technologie zum Selbstschutz des Antiviren-Programms vor Schadprogrammen*
- *Isolierung verdächtiger Objekte in einem speziellen Speicher*
- *Automatisches Update der Datenbanken*

Kaspersky Enterprise Space Security

Das Produkt umfasst Komponenten zum Schutz von Workstations und Groupware-Servern vor allen aktuellen Internet-Gefahren. Viren werden aus dem E-Mail-Datenstrom gelöscht. Die Integrität der Daten sowie die schnelle und sichere Verfügbarkeit der Netzwerkressourcen werden gewährleistet.

Vorzüge und Funktionen:

- Schutz für Workstations und Server vor Viren, Trojanern und Würmern
- Schutz der Mailserver Sendmail, Qmail, Postfix und Exim
- Untersuchung aller E-Mails auf einem Microsoft Exchange Server, einschließlich der gemeinsamen Ordner
- Bearbeitung von E-Mails, Datenbanken und anderen Objekten auf Lotus Notes/Domino-Servern
- Schutz vor Phishing-Angriffen und Spam
- Verhinderung von massenhaften E-Mails und Viren-Epidemien
- Skalierbarkeit im Rahmen der verfügbaren Systemressourcen

- Remote-Administration des Produkts, einschließlich zentraler Installation, Konfiguration und Steuerung
- Unterstützung von Cisco® NAC (Network Admission Control);
- Proaktiver Schutz für Workstations vor neuen Schadprogrammen, die noch nicht in die Datenbanken aufgenommen wurden.
- Personal Firewall mit IDS/IPS-System
- Schutz bei der Arbeit in Wi-Fi-Netzwerken
- Untersuchung des Internet-Traffics in Echtzeit
- Rollback-Funktion für schädliche Veränderungen im System
- Dynamisches Ressourcen-Management bei der vollständigen Untersuchung des Systems
- Isolierung verdächtiger Objekte in einem speziellen Speicher
- Berichtssystem über den Status des Schutzsystems
- Automatisches Update der Datenbanken

Kaspersky Total Space Security

Diese Lösung überwacht alle ein- und ausgehenden Datenströme, E-Mails, Internet-Traffic und alle Netzwerkaktionen. Kaspersky Total Space Security umfasst Komponenten zum Schutz von Workstations und mobilen Geräten, gewährleistet den schnellen und sicheren Zugriff der Anwender auf die Informationsressourcen der Firma und auf das Internet. Außerdem garantiert es Sicherheit bei der Kommunikation per E-Mail.

Vorzüge und Funktionen:

- *Komplexer Schutz vor Viren, Spyware, Hackerangriffen und Spam* auf allen Ebenen eines Unternehmensnetzwerks von der Workstation bis zur Internet-Gateway.
- *Proaktiver Schutz* für Workstations vor neuen Schadprogrammen, die noch nicht in die Datenbanken aufgenommen wurden.
- *Schutz für Mailserver und Groupware-Server*
- *Echtzeit-Untersuchung des Internet-Datenverkehrs* (HTTP/FTP), der in ein lokales Netzwerk eintrifft.
- *Skalierbarkeit im Rahmen der verfügbaren Systemressourcen*
- *Sperren des Zugriffs auf infizierte Workstations*
- *Verhinderung von Viren-Epidemien*

- *Zentrale Berichte über den Schutzstatus*
- *Remote-Administration* des Produkts, einschließlich zentraler Installation, Konfiguration und Steuerung
- *Unterstützung von Cisco® NAC* (Network Admission Control);
- *Unterstützung von Hardware-Proxyservern*
- *Filterung des Internet-Datenverkehrs* nach einer Liste vertrauenswürdiger Server, nach Objekttypen und nach Benutzergruppen
- *Verwendung der iSwift-Technologie zur Vermeidung wiederholter Untersuchungen* innerhalb eines Netzwerks
- *Dynamisches Ressourcen-Management* bei der vollständigen Untersuchung des Systems
- *Personal Firewall* mit IDS/IPS-System
- *Sichere Arbeit in Netzwerken aller Typen*, einschließlich Wi-Fi
- *Schutz vor Phishing-Angriffen und Spam*
- *Möglichkeit zur Remote-Reparatur* (Intel® Active Management - Intel® vPro™)
- *Rollback-Funktion für schädliche Veränderungen im System*
- *Technologie zum Selbstschutz des Antiviren-Programms vor Schadprogrammen*
- *Vollständige Unterstützung von 64-Bit-Betriebssystemen*
- *Automatisches Update der Datenbanken*

Kaspersky Security für Mail-Server

Kaspersky Security für Mail-Server schützt Mailserver und Groupware-Server gegen Schadprogramme und Spam. Das Produkt umfasst Anwendungen für den Schutz aller bekannten Mailserver wie Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix und Exim. Zudem kann auch ein separater Mail-Gateway organisiert werden. Zu dieser Lösung gehören:

- Kaspersky Administration Kit
- Kaspersky Mail Gateway
- Kaspersky Anti-Virus for Lotus Notes/Domino
- Kaspersky Anti-Virus for Microsoft Exchange
- Kaspersky Anti-Virus for Linux Mail Server

Funktionen:

- Zuverlässiger Schutz vor schädlichen und potenziell gefährlichen Programmen
- Spam-Filterung
- Scan von ein- und ausgehenden E-Mails und E-Mail-Anhängen
- Antiviren-Untersuchung aller E-Mails auf einem Microsoft Exchange Server, einschließlich der gemeinsamen Ordner
- Untersuchung von E-Mails, Datenbanken und anderen Objekten auf Lotus Notes/Domino-Servern
- Filterung von E-Mails nach Typen der Anhänge
- Isolierung verdächtiger Objekte in einem speziellen Speicher
- Komfortable Bedienung
- Verhinderung von Viren-Epidemien
- Monitoring für den Status des Schutzsystems mit Hilfe von Benachrichtigungen
- Berichtsystem über die Arbeit der Anwendung
- Skalierbarkeit im Rahmen der verfügbaren Systemressourcen
- Automatisches Update der Datenbanken

Kaspersky Security für Internet-Gateway

Das Produkt gewährleistet allen Mitarbeitern eines Unternehmens den sicheren Zugriff auf das Internet. Die Lösung löscht automatisch alle schädlichen und potenziell gefährlichen Programme aus dem Datenstrom, der über die Protokolle HTTP und FTP eintrifft. Das Produkt umfasst:

- Kaspersky Administration Kit
- Kaspersky Anti-Virus for Proxy Server
- Kaspersky Anti-Virus for Microsoft ISA Server
- Kaspersky Anti-Virus for Check Point FireWall-1

Funktionen:

- Zuverlässiger Schutz vor schädlichen und potenziell gefährlichen Programmen
- Echtzeit-Untersuchung des Internet-Datenverkehrs (HTTP/FTP)

- Filterung des Internet-Datenverkehrs nach einer Liste vertrauenswürdiger Server, nach Objekttypen und nach Benutzergruppen
- Isolierung verdächtiger Objekte in einem speziellen Speicher
- Komfortable Bedienung
- Berichtsystem über die Arbeit der Anwendung
- Unterstützung von Hardware-Proxyservern
- Skalierbarkeit im Rahmen der verfügbaren Systemressourcen
- Automatisches Update der Datenbanken

Kaspersky® Anti-Spam

Kaspersky Anti-Spam ist die erste in Russland entwickelte Software zum Spam-Schutz von kleinen und mittleren Unternehmen. Das Programm vereint moderne Verfahren der Sprachanalyse für Informationen in Textform, sämtliche modernen Verfahren zum Filtern von E-Mails (einschließlich RBL-Listen und formeller Prüfung von Nachrichten) sowie eine einmalige Auswahl an Dienstprogrammen, durch die der Nutzer in die Lage versetzt wird, bis zu 95 % der unerwünschten Nachrichten zu identifizieren und zu eliminieren.

Kaspersky® Anti-Spam ist ein Filterprogramm, das, am "Eingang" des firmeninternen Netzwerks installiert, sämtliche eingehenden E-Mails auf Spam überprüft. Das Programm ist kompatibel mit jedem beliebigen Mailing-System und kann sowohl auf bereits funktionierenden als auch auf separaten Mailservern installiert werden.

Die tägliche Aktualisierung der Filterdatenbank mit Mustertexten aus unserem Sprachlabor garantiert eine hohe Effizienz des Produkts. Die Datenbank-Updates erscheinen alle 20 Minuten.

Kaspersky Anti-Virus® for MIMESweeper

Kaspersky Anti-Virus® for MIMESweeper bietet die Hochgeschwindigkeits-Antiviren-Untersuchung des Datenverkehrs auf Servern, die Clearswift MIMEsweeper for SMTP / Clearswift MIMEsweeper for Exchange / Clearswift MIMEsweeper for Web verwenden.

Das Programm besitzt die Form eines Plug-Ins (Erweiterungsmoduls) und führt im Echtzeit-Modus die Antiviren-Untersuchung und die Bearbeitung der ein- und ausgehenden E-Mail-Nachrichten durch.

C.2. Kontaktinformationen

Sollten Sie weitere Informationen wünschen, wenden Sie sich bitte an unsere Vertriebspartner oder direkt an Kaspersky Lab. Wir werden Sie gern umfassend per Telefon oder E-Mail beraten.

Weitere Information erhalten Sie bei:

Kaspersky Labs GmbH

Steinheilstraße 13

85053 Ingolstadt

Technischer Support	E-Mail: support@kaspersky.de
Allgemeine Informationen	http://www.kaspersky.de/ http://www.viruslist.de/
Feedback zu unseren Benutzerhandbüchern	docfeedback@kaspersky.com (Diese Adresse ist für Rückmeldungen über das Handbuch und elektronische Hilfesystem gedacht.)

SACHREGISTER

ANHANG D. ENDBENUTZER-LIZENZVERTRAG

Endbenutzer-Lizenzvertrag für die erworbene KASPERSKY LAB SOFTWARE

WICHTIG - bitte sorgfältig lesen: Lesen Sie die in diesem KASPERSKY LAB Endbenutzer-Lizenzvertrag ("EULA") beschriebenen Rechte und Einschränkungen sorgfältig durch. Sie werden gebeten, die Bestimmungen des EULAs zu prüfen und ihnen zuzustimmen oder diese abzulehnen.

Indem Sie das Sicherheitsetikett auf der CD-Box aufreißen oder wenn Sie die SOFTWARE installieren, erklären Sie sich mit den Bestimmungen des EULAs einverstanden. Falls Sie mit den Bestimmungen des EULAs NICHT einverstanden sind, geben Sie die erworbene Software bitte innerhalb von 14 Tagen an die Einkaufsstelle zurück. Nach Eingabe des Aktivierungscodes ist eine Rückgabe der Software ausgeschlossen.

Jede Bezugnahme auf "Software" schließt den Aktivierungscode oder die Schlüsseldatei ein, den Sie von Kaspersky Lab als Teil der Software erhalten.

Dieser EULA ist ein rechtsgültiger Vertrag zwischen Ihnen, dem Besitzer eines Exemplars der SOFTWARE (entweder als natürlicher oder als juristischer Person) und KASPERSKY LAB. KASPERSKY LAB wird sich das exklusive Urheberrecht auf die Computersoftware (auf die Software und die Antiviren-Datenbanken) vorbehalten. Indem Sie die SOFTWARE installieren, erklären Sie sich damit einverstanden, durch die Bestimmungen dieses EULAs gebunden zu sein. Falls Sie den Bestimmungen dieses EULAs nicht zustimmen, sind Sie nicht berechtigt, die SOFTWARE zu installieren und zu verwenden.

Die SOFTWARE ist sowohl durch Urheberrechtsgesetze und internationale Urheberrechtsverträge als auch durch andere Gesetze und Vereinbarungen über geistiges Eigentum geschützt. Die SOFTWARE wird lizenziert, nicht verkauft.

1. LIZENZEINRÄUMUNG. Durch diesen EULA werden Ihnen folgende Rechte eingeräumt:

- Sie sind berechtigt, eine Kopie der SOFTWARE auf einem einzigen Computer zu installieren und zu verwenden. Eine Mehrplatzlizenz der SOFTWARE, dürfen Sie auf so vielen Computern installieren, wie Sie Lizenzen erworben haben.

- Sie sind berechtigt, die installierte SOFTWARE innerhalb der erworbenen Lizenzdauer zu benutzen.

2. EINSCHRÄNKUNGEN

• Einschränkungen im Hinblick auf Zurückentwicklung (Reverse Engineering), Dekompilierung und Disassemblierung. Sie sind nicht berechtigt, die SOFTWARE zurückzuentwickeln (Reverse Engineering), zu dekompilieren oder zu disassemblieren, es sei denn und nur insoweit, wie das anwendbare Recht, ungeachtet dieser Einschränkung, dies ausdrücklich gestattet. Sie sind nicht berechtigt, diese Software in automatischen, halbautomatischen oder manuellen Tools zu verwenden, welche dazu dienen, Virensignaturen, Virenerkennungsroutinen, sowie beliebige andere Daten oder Codes zum Erkennen von schädlichem Code oder Daten zu erstellen.

• Vermietung. Sie sind nicht berechtigt, die SOFTWARE zu vermieten, zu verleasen oder zu verleihen.

• Supportleistungen. Nach Kauf und Aktivierung der SOFTWARE erhalten Sie sofort das Recht auf die Supportleistungen für die Lizenzdauer. Supportleistungen verstehen sich wie folgt:

– stündliche Updates der Antiviren-Datenbank

– kostenloses Updates der Software

– kostenlose technische Unterstützung sowohl per e-Mail als auch per Telefon mit KASPERSKY LAB

3. KÜNDIGUNG. Unbeschadet sonstiger Rechte ist KASPERSKY LAB berechtigt, diesen EULA zu kündigen, sofern Sie gegen die Bestimmungen dieses EULAs verstoßen. In einem solchen Fall sind Sie verpflichtet, sämtliche Kopien der SOFTWARE und alle ihre Komponenten zu vernichten.

4. URHEBERRECHT. Eigentum und Urheberrecht auf die SOFTWARE, die gedruckten Begleitmaterialien und jede Kopie der SOFTWARE liegen bei KASPERSKY LAB.

5. GEWÄHRLEISTUNG. KASPERSKY LAB gewährleistet, dass:

• die SOFTWARE den Spezifikationen im wesentlichen entspricht.

• im Falle einer physikalischen Lieferung der Originaldatenträger frei von Material- und Herstellungsfehlern ist.

• das Programm korrekt auf den Datenträger aufgezeichnet ist, die Dokumentation sämtliche Informationen enthält, die KASPERSKY LAB für die Benutzung der Software für erforderlich hält.

• die SOFTWARE binnen 90 Tagen ab der ersten Installation oder dem ersten Download, falls richtig behandelt, der in der beiliegenden Dokumentation bestimmten Funktionalität entspricht und laut derer voll funktionsfähig ist.

Gewährleistungspflichtige Mängel werden von KASPERSKY LAB oder dessen Lieferanten nach Entdeckung, auf jeden Fall aber vor Ablauf von der Gewährleistungsfrist, dem Ermessen von Kaspersky Lab nach, durch Ersatz, Reparatur, Umtausch oder Rückzahlung beseitigt, falls eine Mangelrüge rechtzeitig an Kaspersky Lab oder dessen Lieferanten gerichtet wurde. KASPERSKY LAB oder dessen Lieferanten übernehmen keine Gewährleistung für Mängel, die auf andere als für die Software vorgesehenen Einsatzbedingungen, unsachgemäße Behandlung oder dergleichen zurückzuführen sind.

ALLE ANDERE GEWÄHRLEISTUNGEN UND BEDINGUNGEN, SEIEN SIE AUSDRÜCKLICH ODER KONKLUDENT, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF, (FALLS ZUTREFFEND) JEDE KONKLUDENTE GEWÄHRLEISTUNG IM HINBLICK AUF HANDELSÜBLICHKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, FAHRLÄSSIGKEIT ODER MANGELNDE FACHMÄNNISCHE BEMÜHUNGEN WERDEN VON KASPERSKY LAB ODER DESSEN LIEFERANTEN ABGELEHNT. ES BESTEHT EBENFALLS KEINE GEWÄHRLEISTUNG ODER BEDINGUNG VON RECHTSANSPRÜCHEN IN BEZUG AUF RECHTSINHABERSCHAFT, UNGESTÖRTES NUTZUNGVERGNÜGEN ODER NICHTVERLETZUNG VON RECHTEN DRITTER. DAS GESAMTE RISIKO, DAS BEI DER BENUTZUNG ODER LEISTUNG DER SOFTWARE ENTSTEHT, LIEGT BEI IHNEN.

6. AUSSCHLUSS DER HAFTUNG FÜR ALLE SCHÄDEN. SOWEIT GESETZLICH ZUGELASSEN, SIND KASPERSKY LAB ODER DESSEN LIEFERANTEN IN KEINEM FALL HAFTBAR FÜR IRGENDWELCHE FOLGE-, ZUFÄLLIGEN, DIREKTEN, INDIREKTEN, SPEZIELLEN, STRAFRECHTLICHEN ODER ANDEREN SCHÄDEN WELCHER ART AUCH IMMER (EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF SCHÄDEN AN PERSONEN ODER SACHEN, SCHÄDEN AUS ENTGANGENEM GEWINN, GESCHÄFTSUNTERBRECHUNG, VERLUST VON GESCHÄFTLICHEN INFORMATIONEN, FÜR DEN VERLUST VON PRIVATSPHÄRE, DIE UNMÖGLICHKEIT, EINE PFLICHT ZU ERFÜLLEN (EINSCHLIESSLICH GEMÄSS TREU UND GUTEN GLAUBENS ODER VERNÜNFTIGER ANGEMESSENER SORGFALT) ZU ERFÜLLEN, FÜR FAHRLÄSSIGKEIT ODER ANDERE VERMÖGENSSCHÄDEN), DIE AUS DER VERWENDUNG DER SOFTWARE ODER DER TATSACHE, DASS SIE NICHT VERWENDET WERDEN KANN, RESULTIEREN ODER DAMIT IN ZUSAMMENHANG STEHEN, SELBST WENN KASPERSKY LAB ODER DESSEN LIEFERANTEN AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WORDEN IST. DIESER HAFTUNGSAUSSCHLUSS FÜR SCHÄDEN GILT AUCH DANN, WENN ABHILFEMASSNAHMEN IHREN WESENTLICHEN ZWECK VERFEHLEN.

7. ANWENDBARES RECHT. Dieser Vertrag unterliegt der Gesetzgebung des Landes, indem das Produkt erworben wurde.